

VMware™

User's Manual

# ESX Server™

Version 1.5

**VMware, Inc.**

3145 Porter Drive  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**Please note that you will always find the most up-to-date technical documentation on our Web site at <http://www.vmware.com/support/>.**

**The VMware Web site also provides the latest product updates.**

© 2002 VMware, Inc. All rights reserved. VMware, the VMware boxes logo, MultipleWorlds, GSX Server and ESX Server are trademarks of VMware, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. IBM, xSeries, ServerProven and the e-business logo are trademarks of the International Business Machines Corporation. Linux is a registered trademark of Linus Torvalds. All other marks and names mentioned herein may be trademarks of their respective companies. Rev: 20021205 Item: ESX-Q202-004

# Table of Contents

<b>Introduction and System Requirements</b>	<b>11</b>
Introduction and System Requirements	12
Welcome to VMware ESX Server	13
How VMware ESX Server Works	13
What's New in Version 1.5	15
System Requirements	17
Server Hardware Requirements	17
Remote Management Workstation Requirements	19
Supported Guest Operating Systems	20
Virtual Machine Specifications	20
Legacy Devices	21
Technical Support Resources	22
The VMware Web Site	22
VMware Newsgroups	22
Reporting Problems	22
<b>Installing, Configuring and Upgrading ESX Server</b>	<b>25</b>
Installing, Configuring and Upgrading ESX Server	26
Installing the Software on the Server	28
Before You Begin	28
Installing VMware ESX Server	28
Using the Setup Wizard to Configure Your Server	33
Configuring Storage for Virtual Machine Files	45
Creating a New Virtual Machine	59
Installing a Guest Operating System and VMware Tools	70
Installing a Guest Operating System in a Virtual Machine	70
Migrating VMware Workstation and VMware GSX Server Virtual Machines	71
Installing VMware Tools and the Network Driver in the Guest Operating System	73
Preparing to Use the Remote Management Software	79
Registering Your Virtual Machines	79
Installing the Remote Console Software	81
Windows XP, Windows 2000 or Windows NT 4.0	81
Linux – RPM Installer	81
Linux – Tar Installer	81

Accepting the Security Certificate from ESX Server	83
Microsoft Internet Explorer 5.5	83
Netscape Navigator 4.7x on a Windows Management Workstation	84
Installing Additional Hardware on the Server	86
Installing Hardware for Use by Virtual Machines	86
Installing Hardware for Use by the Console Operating System	86
Upgrading from a Previous Version of ESX Server	87
Before You Install ESX Server 1.5	87
Upgrading from ESX Server 1.1 to ESX Server 1.5	88
Upgrading from ESX Server 1.0 to ESX Server 1.5	88
Setting File Permissions on Existing Virtual Disk Files	89
Updating Virtual Machine Configurations	90
<b>Running VMware ESX Server</b>	<b>91</b>
Running VMware ESX Server	92
Using the VMware Management Interface	94
Editing a Virtual Machine's Configuration Remotely	99
Managing the VMware ESX Server File System from the Management Interface	99
Viewing and Changing VMkernel Settings	104
Deleting a Virtual Machine from the Management Interface	106
Using Disk Modes	108
Monitoring System Status	109
Setting the MIME Type in Netscape Navigator 4.x	111
Setting the MIME Type in Netscape 6 and Mozilla	112
Using the Remote Console	114
Starting the Remote Console on Windows	114
Starting the Remote Console on Linux	114
Running a Virtual Machine Using the Remote Console	115
VMware Tools Settings	117
Installing New Software Inside the Virtual Machine	119
Cutting, Copying and Pasting	119
Suspending and Resuming Virtual Machines	120
Shutting Down a Virtual Machine	121
Rebooting or Shutting Down the Server	122
Using SNMP with ESX Server	125
Using SNMP to Monitor the Computer Running ESX Server	125
Installing and Running the ESX Server SNMP Agent	127

Configuring the ESX Server SNMP Agent .....	129
Configuring SNMP Management Software .....	131
Configuring SNMP Security .....	132
Using SNMP with Guest Operating Systems .....	132
VMware ESX Server SNMP Variables .....	132
Backing Up Virtual Machines .....	140
Using Tape Drives with VMware ESX Server .....	140
Backing Up from within a Virtual Machine .....	140
Backing Up Virtual Machines from the Console Operating System .....	141
Using Hardware or Software Disk Snapshots .....	142
Using Network-based Replication Tools .....	143
The VMware Guest Operating System Service .....	144
Synchronizing the Time Between the Guest and Console Operating Systems .....	144
Shutting Down and Restarting a Virtual Machine .....	145
Executing Commands When ESX Server Requests the Guest Service to Halt or Reboot a Virtual Machine .....	146
Passing a String from the Console Operating System to the Guest Operating System .....	147
<b>Guest Operating Systems .....</b>	<b>149</b>
Guest Operating Systems .....	150
Installing Guest Operating Systems .....	151
Windows 2000 Installation Guidelines .....	152
Windows NT Installation Guidelines .....	153
Red Hat Linux 7.3 Installation Guidelines .....	154
Red Hat Linux 7.1 and 7.2 Installation Guidelines .....	156
Red Hat Linux 7.0 Installation Guidelines .....	158
Red Hat Linux 6.2 Installation Guidelines .....	160
SuSE Linux 7.3 Installation Guidelines .....	162
FreeBSD 4.5 Installation Guidelines .....	164
The VMware Guest Operating System Service .....	167
<b>Console Operating System and VMkernel .....</b>	<b>169</b>
Console Operating System and VMkernel .....	170
Characteristics of the VMware Console Operating System .....	171
Using DHCP for the Console Operating System .....	171
Loading and Unloading the VMkernel .....	173
The VMkernel Loader .....	173

Configuring Your Server to Use VMkernel Device Modules	174
Loading VMkernel Device Modules	174
VMkernel Module Loader	174
Other Information about VMkernel Modules	177
<b>Configuring and Running Virtual Machines</b>	<b>179</b>
Configuring and Running Virtual Machines	180
Configuring Virtual Machines	181
Using VMkernel Devices	182
Recommended Configuration Options	186
Modifying the SMBIOS UUID	187
Suspending and Resuming Virtual Machines	190
Setting the Suspend Directory	190
Enabling Repeatable Resumes	191
Authentication and Security Features	193
Authenticating Users	193
Default Permissions	194
TCP/IP Ports for Management Access	194
<b>Disks</b>	<b>197</b>
Disks	198
File System Management on SCSI Disks and RAID	199
Using vmkfstools	199
Naming VMFS File Systems	205
Mounting VMFS File Systems on the Console Operating System	205
Utility to Mount VMFS File Systems	206
Determining SCSI Target IDs	208
Sharing the SCSI Bus	210
Setting Bus Sharing Options	210
Using Storage Area Networks with ESX Server	212
Detecting All LUNs	212
Special Options for SAN Configurations	212
<b>Networking</b>	<b>215</b>
Networking	216
Setting the MAC Address Manually for a Virtual Machine	217
How VMware ESX Server Generates MAC Addresses	217
Setting MAC Addresses Manually	218

The VMkernel Network Card Locator .....	220
Forcing the Network Driver to Use a Specific Speed .....	221
Forcing a Virtual Adapter to Use Promiscuous Mode .....	222
Sharing Network Adapters and Virtual Networks .....	224
Allowing the Console Operating System to Use the Virtual Machines’ Devices .....	224
Starting Shared VMkernel Network Adapters and Virtual Networks when the Console Operating System Boots .....	225
Sharing the Console Operating System’s Network Adapter with Virtual Machines .....	226
Performance Tuning for Heavy Network Loads .....	228
Enabling Interrupt Clustering .....	228
Interrupt Clustering Parameters .....	228
<b>Resource Management .....</b>	<b>231</b>
Resource Management .....	232
CPU Resource Management .....	234
Proportional-share Scheduling .....	234
Multiprocessor Systems .....	235
Managing CPU Resources from the Management Interface .....	236
Managing CPU Resources from the Console Operating System .....	236
Memory Resource Management .....	239
Allocation Parameters .....	239
Admission Control .....	240
Dynamic Allocation .....	240
Memory Reclamation .....	241
Memory Sharing .....	242
Managing Memory Resources from the Management Interface .....	243
Managing Memory Resources with Configuration File Settings .....	243
Console Operating System Commands .....	244
Sizing Memory on the Server .....	249
Server Memory .....	249
Console Operating System Memory .....	249
Virtual Machine Memory Pool .....	249
Virtual Machine Memory .....	250
Memory Sharing .....	250
Memory Overcommitment .....	251
Example: Web Server Consolidation .....	251

More Information _____	252
Network Bandwidth Management _____	253
Using Network Filters _____	253
Managing Network Bandwidth from the Management Interface _____	253
Managing Network Bandwidth from the Console Operating System _____	254
Traffic Shaping with nftshaper _____	254
Disk Bandwidth Management _____	257
Allocation Policy _____	257
Managing Disk Bandwidth from the Management Interface _____	258
Configuration File Options _____	258
Managing Disk Bandwidth from the Console Operating System _____	259
<b>Glossary _____</b>	<b>261</b>
Glossary _____	262
<b>Appendix A: I/O Adapter Compatibility Guide _____</b>	<b>265</b>
I/O Adapter Compatibility Guide _____	266
Currently Supported Device Families _____	266
Linux Driver Compatibility _____	267
VMware Certification _____	267
Adaptec SCSI Adapters _____	268
Mylex (Buslogic) SCSI Adapters _____	269
LSI Logic (Symbios, NCR) Based SCSI Adapters _____	270
Emulex Fibre Channel Adapters _____	272
QLogic Fibre Channel Adapters _____	272
Compaq RAID Controllers _____	272
Dell PercRAID RAID Controllers _____	273
IBM ServeRAID RAID Controllers _____	273
Mylex DAC960 RAID Controllers _____	273
Intel EEPro Family Ethernet NICs _____	273
3Com EtherLink PCI III/XL Series Ethernet NICs _____	276
Alteon AceNIC and Compatible Gigabit Ethernet NICs _____	276
Broadcom Gigabit Ethernet NICs _____	277
Intel Gigabit Ethernet NICs _____	277
<b>Appendix B: The OpenSSL Toolkit License _____</b>	<b>279</b>
The OpenSSL Toolkit License _____	280
License Issues _____	280
OpenSSL License _____	280



Original SSLeay License \_\_\_\_\_ 281

**Index** \_\_\_\_\_ **283**



# 1

## **Introduction and System Requirements**

# Introduction and System Requirements

The following sections introduce VMware ESX Server and list the requirements for running it on a server:

- [Welcome to VMware ESX Server on page 13](#)
- [System Requirements on page 17](#)
  - [Server Hardware Requirements on page 17](#)
  - [Supported Guest Operating Systems on page 20](#)
  - [Remote Management Workstation Requirements on page 19](#)
- [Technical Support Resources on page 22](#)
  - [The VMware Web Site on page 22](#)
  - [VMware Newsgroups on page 22](#)
  - [Reporting Problems on page 22](#)

# Welcome to VMware ESX Server

Thank you for choosing VMware™ ESX Server™, the virtual machine software for consolidating and partitioning servers in high-performance environments. It is a cost-effective, highly scalable virtual machine platform with advanced resource management capabilities.

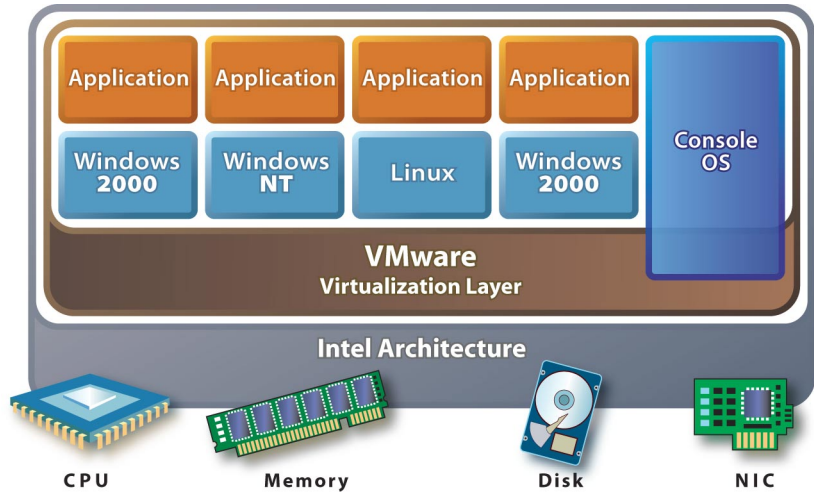
Ideally suited for corporate IT and service provider data centers, VMware ESX Server lets you minimize the total cost of ownership of server infrastructure by maximizing server manageability, flexibility and efficiency across the enterprise.

VMware ESX Server allows you to

- Implement server consolidation. You can consolidate applications and infrastructure services onto fewer highly scalable, highly reliable enterprise-class servers.
- Deliver high availability and provide for disaster recovery. With a stable, uniform platform, you can deliver more services and deploy new solutions faster and more efficiently. You can store critical data in secure, isolated virtual servers to protect against the vulnerabilities of physical servers.
- Guarantee service levels. Like an internal service provider, your IT department can deliver guaranteed server resources of CPU, memory, disk bandwidth and network bandwidth at optimum performance levels, improving service to customers.
- Streamline development and testing. Your software developers and quality assurance engineers can work effectively with multiple machine environments and build more realistic tests in less time with less hardware.

## How VMware ESX Server Works

VMware ESX Server simplifies server infrastructure by partitioning and isolating server resources, enabling you to manage these resources remotely and to automate and standardize them.



ESX Server lets you transform physical computers into a pool of logical computing resources. You can partition physical servers into secure virtual machine servers. You isolate your operating systems and applications in these multiple virtual machine servers that reside on a single piece of hardware. You can then distribute these resources to any operating system or application as needed, when needed, giving you mainframe-class control of your server infrastructure.

The operating system running inside a virtual machine is called a guest operating system.

# What's New in Version 1.5

## **Scale to the Largest Server Platforms**

VMware ESX Server now supports up to 64 concurrent virtual machines with adequate memory and storage resources.

ESX Server now supports the PAE (physical address extension) standard for larger memory on the physical computer. This version supports system memory up to 64GB of RAM.

This release also has support for additional Gigabit Ethernet network cards.

## **Consolidate Even the Most Memory-intensive Applications**

VMware ESX Server can now provision up to 3.6GB of RAM per virtual machine

## **Intensify Resource Utilization**

Advanced memory management techniques enable you to configure and run virtual machines with total memory greater than the amount of physical RAM on the system. It can be equivalent to putting up to 64GB of additional RAM into your system.

New resource management tools enable you to regulate the amount of disk I/O bandwidth used by each virtual machine.

## **Enjoy IBM ServerProven Certification**

VMware ESX Server has passed the rigorous tests for IBM® ServerProven® certification on the IBM eServer xSeries 330, xSeries 350, xSeries 360, xSeries 370 and xSeries 440 server platforms.

## **Manage Systems More Easily**

You can now perform an expanded range of management tasks from the VMware Management Interface, instead of logging in to the console operating system and executing commands at the command line.

## **Monitor Servers and Virtual Machines with Standard Tools**

Take advantage of IBM Director management software on your eServer xSeries systems. Or use Compaq Insight Manager, HP OpenView or another compatible SNMP management application to track the configuration and health of the server and its virtual machines.

## **Accomplish More Management Tasks from Your Workstation**

The expanded VMware Management Interface enables you to monitor and manage your server and virtual machines more effectively using a Web browser and a secure SSL connection between your management workstation and the server. SSH support

gives you the option of running a secure terminal application to carry out command line tasks remotely.

### **Control Access to Virtual Disk Files**

Access controls enable you to determine which users have access to virtual disk files stored on VMFS partitions.



# System Requirements

## Server Hardware Requirements

### Minimum

- Processor: Intel® Pentium® II 500MHz and above
- 512MB RAM minimum
- Two or more Ethernet adapters. Supported adapters include:
  - 3Com® adapters
  - Alteon AceNIC-based adapters
  - Broadcom® BCM5700-based adapters
  - Intel Pro/100 adapter
  - Intel PRO/1000 server adapters

**Note:** For best performance and security, separate Ethernet adapters should be used for the console operating system and the virtual machines. It is also possible to use just one Ethernet adapter, shared between the console operating system and the virtual machines. For details, see [Sharing Network Adapters and Virtual Networks on page 224](#).

- A SCSI adapter, Fibre Channel adapter or internal RAID controller.

The basic SCSI adapters supported are Adaptec®, BusLogic® and most NCR™/Symbios™ SCSI adapters. The SCSI RAID adapters supported are Compaq® Smart Array, Dell® PercRAID (Adaptec RAID and AMI MegaRAID), IBM® ServeRAID™ and Mylex® SCSI RAID devices. The Fibre Channel adapters that are supported are Emulex™ and QLogic™ adapters.
- A SCSI disk or RAID LUN with unpartitioned space. In a minimum configuration, this disk or RAID is shared between the console operating system and the virtual machines.

### Recommended for Enhanced Performance

- A second disk controller with one or more drives.

The lists above outline a basic configuration. In practice, you may use multiple physical disks, which may be SCSI disks, Fibre Channel disks or RAID LUNs. For best performance, all of the data used by the virtual machines should be on the physical disks allocated to virtual machines. Therefore, these physical disks should be large enough to hold disk images that will be used by all the virtual machines.

Similarly, you should provide enough RAM for all of the virtual machines plus the console operating system. For background on the console operating system, see [Characteristics of the VMware Console Operating System on page 171](#). For details on how to calculate the amount of RAM you need, see [Sizing Memory on the Server on page 249](#).

**Note:** To ensure the best possible I/O performance and workload management, VMware ESX Server provides its own drivers for supported devices. Be sure that the devices you plan to use in your server are supported. For additional detail on I/O device compatibility, download the VMware ESX Server I/O Adapter Compatibility Guide from the VMware Web site at [www.vmware.com/pdf/esx\\_io\\_devices\\_15.pdf](http://www.vmware.com/pdf/esx_io_devices_15.pdf).

ESX Server virtual machines can share an Ethernet card with the console operating system as described in [Sharing Network Adapters and Virtual Networks on page 224](#). For best performance, however, you should configure the virtual machines to use an Ethernet card separate from the one used by the console operating system.

ESX Server virtual machines can share a SCSI disk with the console operating system, but for enhanced disk performance, you can configure the virtual machines to use a SCSI adapter and disk separate from those used by the console operating system. You should make sure enough free disk space is available to install the guest operating system and applications for each virtual machine on the disk that they will use.

### Maximum Physical Machine Specifications

- 8 processors per system
- 64GB of RAM per system
- 64 adapters of all types, including storage and network adapters, per system
- 16 physical Ethernet adapters per system
- Up to 4 Gigabit Ethernet adapters, or up to 16 10/100 Ethernet adapters per system
- 64 virtual machines per system
- 256 files per VMFS partition

### Remote Management Workstation Requirements

The remote workstation is a Windows NT 4.0, Windows 2000, Windows XP or Linux system from which you launch a remote console and access the VMware Management Interface. The remote console runs as a standalone application. The VMware Management Interface uses a Web browser.

#### Hardware Requirements

- Standard x86-based computer
- 266MHz or faster processor
- 64MB RAM minimum
- 10MB free disk space required for basic installation

#### Software — Windows Remote Workstation

- Windows XP Home Edition or Professional
- Windows 2000 Professional, Server or Advanced Server
- Windows NT 4.0 Workstation or Server, Service Pack 6a
- The VMware Management Interface is designed for these browsers:
  - Microsoft® Internet Explorer 5.0 or higher
  - Netscape Navigator® 4.5 or higher
  - Netscape® 6
  - Mozilla 0.9.4 or higher

#### Software — Linux Remote Workstation

Compatible with standard Linux distributions with glibc version 2 or higher and one of the following:

- For single-processor systems: kernel 2.0.32 or higher in the 2.0.x series, kernel in the 2.2.x series, or 2.4.x kernel
- For SMP systems: kernel in the 2.2.x series or 2.4.x kernel
- The VMware Management Interface is designed for these browsers:
  - Netscape Navigator 4.5 or higher
  - Netscape 6
  - Mozilla 0.9.4 or higher

### Supported Guest Operating Systems

- Windows® 2000 (any server version)
- Windows NT® 4.0 — Service Pack 4 or higher
- Red Hat™ Linux® 6.2, 7.0, 7.1 or 7.2
- SuSE™ Linux 7.3
- FreeBSD 4.5

**Note:** The standard Linux kernels in Red Hat Linux 6.2 have a bug reported at [www.redhat.com/support/errata/RHBA-2000013-01.html](http://www.redhat.com/support/errata/RHBA-2000013-01.html) that can cause data corruption under heavy memory load. Therefore, the standard Red Hat 6.2 installation should not be used as a guest operating system to run server applications unless it is patched. One way to correct the problem is to recompile the guest Linux kernel with the configuration option CONFIG\_X86\_FX=n.

### Virtual Machine Specifications

Each ESX Server computer can host up to 64 virtual machines with the following capabilities and specifications.

#### Processor

- Intel Pentium II or later, (dependent on system processor)
- One processor per virtual machine on symmetric multiprocessor systems

#### Memory

- Up to 3.6GB per virtual machine

#### SCSI Devices

- Up to 4 virtual SCSI adapters per virtual machine with up to 15 devices per adapter
- 9TB per virtual disk

#### Ethernet Cards

- Up to 4 virtual Ethernet adapters per machine

**Note:** Each virtual machine has a total of 5 virtual PCI slots, therefore the total number of virtual adapters, SCSI plus Ethernet, cannot be greater than 5.

#### Floppy Drives

Up to 2 1.44MB floppy drives (physical drives or floppy image files) per virtual machine

#### CD-ROM

Up to 2 drives (physical drives or ISO image files) per virtual machine

### Legacy Devices

Virtual machines may also make use of the following legacy devices. However, for performance reasons, use of these devices is not recommended.

#### IDE Devices

- Up to 4 IDE devices per virtual machine (virtual or physical drives)
- Up to 128GB per virtual disk

#### Serial (COM) Ports

- Up to 4 serial ports per virtual machine

#### Parallel (LPT) Ports

- Up to 4 LPT Ports per virtual machine

## Technical Support Resources

### The VMware Web Site

The latest technical support and troubleshooting notes are available on the VMware Web site at <http://www.vmware.com/support/>.

### VMware Newsgroups

The VMware newsgroups are primarily forums for users to help each other. You are encouraged to read and post issues, work-arounds and fixes. While VMware personnel may read and post to the newsgroups, they are not a channel for official support. The VMware NNTP news server is at [news.vmware.com](http://news.vmware.com).

The following groups are devoted to ESX Server issues:

*vmware.esx-server.configuration*

*vmware.esx-server.guestos*

*vmware.esx-server.installation*

*vmware.esx-server.misc*

*vmware.esx-server.web-mgmt.misc*

### Reporting Problems

If you have problems while running VMware ESX Server, please submit a support request. Problems may occur either in the VMkernel or in the virtual machines that it hosts.

These guidelines describe the information we need from you to diagnose various types of problems.

- If a virtual machine exits abnormally or crashes, please save the log file (*vmware.log* in the same directory as your *.cfg* file) and any core files (*core* or *vmware-core* in that directory). Provide these to VMware along with the virtual machine's configuration (*.cfg*) file and any other information that might help us to reproduce the problem. In addition, include the contents of */var/log/messages* from the console operating system, since the VMkernel logs informational and error messages in */var/log/messages*. Be sure to include a description of your physical hardware and of the software (operating system and applications) that was running in the virtual machine. Include this information in your support request.

A problem in the VMkernel normally causes the machine to display an error screen for a period of time and then reboot. If you specified a VMware core dump partition when you configured your machine, the VMkernel also

generates a core dump and error log. More serious problems in the VMkernel can freeze the machine without an error screen or core dump.

In either of these cases, describe the steps you took in the period before this failure (including any information listed in point 1 above, if applicable). Include this information in your support request, along with the contents of `/var/log/messages` from the console operating system. Also include the core dump and error log, if any. These can be found in files named `vmkernel-core.<date>` and `vmkernel-log.<date>` in the `/root` directory after you reboot your machine.

Be sure to register your serial number. You may then report your problems using the support request form on the VMware Web site at [www.vmware.com/requestsupport](http://www.vmware.com/requestsupport).





# 2

## **Installing, Configuring and Upgrading ESX Server**

# Installing, Configuring and Upgrading ESX Server

The following sections describe how to install and configure ESX Server:

- [Installing the Software on the Server on page 28](#)
  - [Before You Begin on page 28](#)
  - [Installing VMware ESX Server on page 28](#)
- [Using the Setup Wizard to Configure Your Server on page 33](#)
  - [Configuring Storage for Virtual Machine Files on page 45](#)
- [Creating a New Virtual Machine on page 59](#)
- [Installing a Guest Operating System and VMware Tools on page 70](#)
  - [Installing a Guest Operating System in a Virtual Machine on page 70](#)
  - [Migrating VMware Workstation and VMware GSX Server Virtual Machines on page 71](#)
  - [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#)
- [Preparing to Use the Remote Management Software on page 79](#)
  - [Registering Your Virtual Machines on page 79](#)
- [Installing the Remote Console Software on page 81](#)
  - [Windows XP, Windows 2000 or Windows NT 4.0 on page 81](#)
  - [Linux – RPM Installer on page 81](#)
  - [Linux – Tar Installer on page 81](#)
- [Accepting the Security Certificate from ESX Server on page 83](#)
  - [Microsoft Internet Explorer 5.5 on page 83](#)
  - [Netscape Navigator 4.7x on a Windows Management Workstation on page 84](#)
- [Installing Additional Hardware on the Server on page 86](#)
- [Upgrading from a Previous Version of ESX Server on page 87](#)
  - [Before You Install ESX Server 1.5 on page 87](#)
  - [Upgrading from ESX Server 1.1 to ESX Server 1.5 on page 88](#)
  - [Upgrading from ESX Server 1.0 to ESX Server 1.5 on page 88](#)

- [Setting File Permissions on Existing Virtual Disk Files on page 89](#)
- [Updating Virtual Machine Configurations on page 90](#)

## Installing the Software on the Server

This installation guide steps you through the process of installing and configuring the VMware ESX Server software on your server.

Later sections explain how to create and provision virtual machines, how to manage your virtual machines from a remote workstation and how to work with the advanced features of VMware ESX Server.

**Note:** If you are upgrading from a previous version of ESX Server, the process is much faster and simpler than a complete installation. For details, see [Upgrading from a Previous Version of ESX Server on page 87](#).

### Before You Begin

To install VMware ESX Server, you need

- The VMware ESX Server software CD, which includes the VMware Console Operating System, VMware ESX Server software and remote console software.
- A computer that meets the system requirements for ESX Server. See [System Requirements on page 17](#) for details.

**Note:** If you are installing ESX Server on an IBM eServer xSeries 360 server, be sure you have BIOS version 1.03 or higher. Information on BIOS updates is available on the IBM Web site at [techsupport.services.ibm.com/server/fixes?view=xSeries](http://techsupport.services.ibm.com/server/fixes?view=xSeries).

### Installing VMware ESX Server

The VMware ESX Server installation includes the console operating system, the `vmnixmod` module, the VMkernel and VMkernel modules. The console operating system is based on a modified Red Hat Linux 7.2 installation and is called VMnix. It is used to configure, start and administer VMware virtual machines. The `vmnixmod` module is loaded into the VMnix kernel to facilitate loading and communicating with the VMkernel. The VMkernel manages system hardware and the virtual machines running on the server. Users communicate with the VMkernel via the console operating system.

The VMkernel manages all the operating systems on the machine, including both the console operating system and the operating systems running in each virtual machine. The VMkernel modules provide support for high-performance device I/O and allow run-time addition of functionality to the VMkernel (for example, network traffic filters).

Before you begin, be sure you have the network information you need during installation. You need to know

- The IP address for the server where you are installing ESX Server

## Installing, Configuring and Upgrading ESX Server

- The host name for the server, including the full domain name for the server, if applicable
- The netmask for the server's subnet
- The IP address of the gateway
- The IP address of the name server and, optionally, the addresses of one or two alternate name servers

### Installing the VMware ESX Server Software

1. Make sure the network cable is plugged into the main network adapter, so the installer can properly detect that the machine has a network card.
2. Power on the machine and immediately insert the VMware ESX Server CD in the CD-ROM drive.
3. If necessary, enter the BIOS Setup screen and set the CD-ROM as the first boot device.

**Note:** On some Compaq servers, you must also change a setting in the BIOS to ensure that the BIOS correctly populates the PCI IRQ routing entries in the MPS table. On these systems, press F9 during boot to get into system configuration, choose **Advanced > MPS Table Mode > Full Table APIC**. Save the changes and exit.

After it boots, the machine should display a screen saying, Welcome to the VMware ESX Server Install.

4. If the installation screen does not come up properly, your CD-ROM drive may be having trouble booting from the CD. In this case, boot from a VMware ESX Server boot floppy. Use the following steps to create a boot floppy.

#### Windows System

- Put the ESX Server CD in the CD-ROM drive.
- Put a floppy disk in the floppy drive.
- Bring up a DOS command window.
- Use the `rawrite` program to copy the disk image to the floppy disk. If your CD-ROM drive is not `d:`, substitute the correct drive letter.  
`D:\dosutils\rawrite -f d:\boot.img -d a`

#### Linux System

- Put the ESX Server CD in the CD-ROM drive.

- As root, mount the CD.  
`mount /dev/cdrom /mnt/cdrom`
- Put a floppy disk in the floppy drive.
- Copy the boot image from the CD to the floppy.  
`dd if=/mnt/cdrom/boot.img of=/dev/fd0 bs=1474560 \count=1`

**Note:** The command should all be typed on one line. Do not type the backslash.

Then insert the floppy disk in the floppy drive, reboot and, if necessary, make the floppy drive the first boot device. You should leave the CD in the CD-ROM drive.

5. The first screen of the installer outlines the installation and configuration process. It offers a choice between installing and upgrading.

For a full install, choose **Install**.

If you are upgrading an existing ESX Server computer, see [Upgrading from a Previous Version of ESX Server on page 87](#).

6. You are asked if you have a driver disk provided by VMware for a device that is not handled by drivers in this release of ESX Server.

If you do not have a driver disk, choose **No** and continue with the installation.

If you have a driver disk from VMware, put the driver disk into the floppy drive and choose **Yes**.

7. After the driver disk screen, the installer examines all the hardware to determine if the Ethernet and SCSI devices are compatible with VMware ESX server.

If you see the message **Unknown PCI devices**, there are Ethernet or SCSI PCI devices installed on the machine that are not supported by the console operating system, possibly because they are quite new. Contact VMware with details about the device to determine the current level of support for the device.

If you see the message **PCI devices unusable by virtual machines**, there are Ethernet or SCSI PCI devices installed on the machine that are supported by the console operating system but cannot be used by virtual machines. These devices may be older, lower-performance devices that are not supported by VMware ESX Server.

The next series of steps installs the console operating system.

8. In Disk Setup, choose **Disk Druid**.

If you prefer, and if you are installing the console operating system on a hard drive with at least 1.8GB of space, you may choose **Autopartition**. The automatic partitioning creates a swap partition of 250MB, a `/boot` partition of 50MB and a `/` partition of 1,500MB.

**Note:** If you have disks connected via an Emulex Fibre Channel adapter or a QLogic QLA-2300 Fibre Channel adapter, they may not appear in Disk Druid or fdisk and are not used by Autopartition. They will be visible during configuration of the server, when you assign disk space for storage of virtual machine files.

9. The installer asks you if you want to put the boot loader in the master boot record (MBR) of the boot disk or the boot sector of the first partition of the disk.

In most cases, you should choose the default of installing on the MBR.

However, if you have a Compaq server with Compaq SmartStart utilities, choose the boot sector of the first partition of the disk. On the Compaq server, the MBR contains the code to allow starting the SmartStart utilities using the F10 key. If the F10 key is not pressed, the server will automatically try to boot from the first partition.

10. In Current Disk Partitions, delete any existing partitions.

11. Choose the disk where you want to install the console operating system. It should be your first IDE disk (`hda`), if you have one; otherwise, use your first SCSI disk (`sda`).

12. You typically create three partitions for a Linux installation, using the **New** option.

- The first partition should have a mount point of `/boot`, a size of 50MB and a type of `ext3`.
- The second partition should have no mount point, a size of twice the memory assigned to the console operating system and a type of `swap`. You assign memory to the console operating system in a later step. The default amount, 128MB, is appropriate for managing up to three or four virtual machines. If you plan to use that amount of memory for the console operating system, set the size of the swap file to 256MB.

The default amount of memory reserved for the console operating system — 128MB — is sufficient for managing up to three or four virtual machines. Increase this to 192MB for eight virtual machines, 272MB for 16 virtual machines, 384MB for 32 virtual machines or 512MB for more than 32 virtual machines. For details, see [Sizing Memory on the Server on page 249](#).

- The third partition should have a mount point of `/`, a size of about 1800MB and a type of `ext3`. The third partition holds your root file system, and most of the Linux and console operating system files are installed there.

Respond **OK** when you have created these three partitions, and respond **Yes** to the Save Changes prompt.

**Note:** Do not create partitions on any other disks besides the main boot disk.

13. In Network Configuration, disable `bootp/dhcp` and enter the required network parameters. Setup does not ask for network parameters if you do not have a network card. Initially, only the first Ethernet card is enabled. All other network adapters are disabled.

See [Using DHCP for the Console Operating System on page 171](#) for instructions and cautions on setting up a DHCP-based console operating system.

14. Enter the host name in Hostname Configuration.

**Note:** Be sure to include the full domain name if you are running with domains.

15. At the Time Zone Selection screen, choose your time zone. You can type `U` to move quickly to the US time zones, if appropriate.
16. At the Root Password screen, specify your desired root password. Root is the user name for the administrator. Users with administrator privileges log in with this name when using the VMware Management Interface or the console operating system.

In Add User and User Account Setup, you can add additional user accounts. You need accounts for all users who need to log in to the VMware Management Interface to create or run virtual machines. If you wish, you may add those users at this time. However, you may find it more convenient to add them later with the console operating system's `useradd` command or by copying the `/etc/passwd` file from another machine.

17. The installer then formats the disk and starts installing the packages.
18. The final screen appears, informing you that the installation is complete and you are now ready to start configuring ESX Server.

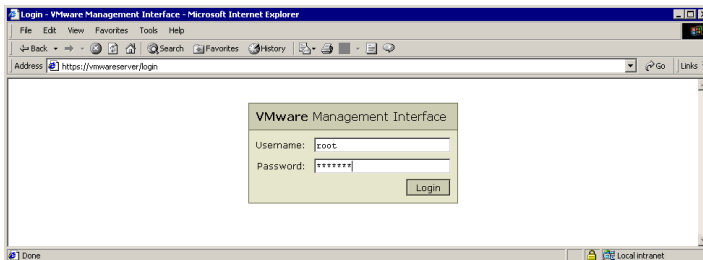


## Using the Setup Wizard to Configure Your Server

A Web-based Setup Wizard guides you through the steps to configure your server. You may return to the wizard at any time to edit your configuration. You may run the Setup Wizard from any computer with network access to your server. Running X on your server's console operating system is not recommended. The steps that follow assume you are using a separate computer as your workstation.

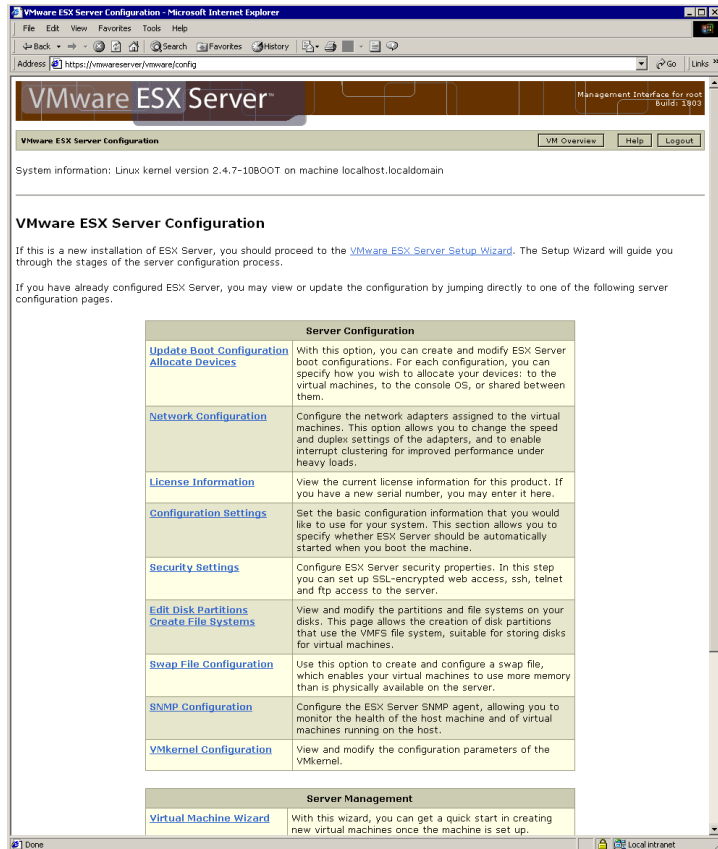
**Note:** If you need secure communications between your management workstations and the server, be sure to choose the appropriate security level when you configure ESX Server. For additional details, see the Network Security section in the technical note [Authentication and Security Features on page 193](#).

1. Launch a supported Web browser (Microsoft Internet Explorer 5.0 or later or Netscape Navigator 4.5 or later) and enter the URL for the VMware Setup Wizard  
`http://<hostname>/`
2. A dialog box asks whether you want to accept the security certificate presented by the server. Accept the certificate. For details, see [Accepting the Security Certificate from ESX Server on page 83](#).



3. Log in as root.

## Installing, Configuring and Upgrading ESX Server



- Start the wizard by clicking the **VMware ESX Server Setup Wizard** link at the top of the page.

System information: Linux kernel version 2.4.7-10BOOT on machine localhost.localdomain

### Boot Configuration

In this section, you can set the basic boot configuration information that you would like to use for your system.

Name of configuration:  
Name must be unique.  
Existing names:

Amount of memory to allocate to the Console:  
Your system is reporting approximately 500 MB of memory.  
If you plan to run 4 virtual machines or fewer, 128 MB should suffice. Set this to 192 MB for 6 virtual machines, 272 MB for 16 virtual machines, or 384 MB for 32 virtual machines, or 512 MB for more than 32 virtual machines.  MB

Name of kernel file to use:  
If you're not sure which setting to choose, it's safe to leave this untouched.

Use as default boot configuration?  
If set as the default, this configuration will be automatically loaded each time you reboot. The current default configuration is **linux**. ☒ Yes

### Device Allocation

For each device, select whether you would like to allocate it to the Console OS, to the Virtual Machines, or share it between the two.

- Console:** Device can only be used by the Console OS and is unavailable to your virtual machines.
- Virtual Machines:** Device can only be used by your virtual machines and is unavailable to the Console OS.
- Shared:** Some devices such as SCSI and RAID adapters can be shared, enabling them to be used by both the Console OS and your virtual machines.

**Important note** — when allocating devices:

- Make sure the Console's active network adapter (typically the first listed network adapter) does not get reassigned to the virtual machines. Otherwise you will lose network connectivity upon rebooting the machine after boot configuration is complete.
- If the Console OS and Virtual Machines will be using disks that reside on the same SCSI/RAID adapter, that adapter must be configured as "Shared."

Console	Shared	Virtual Machines	Device Name	Driver	Bus	Dev
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Ethernet controller: Intel Corporation 82557 [Ethernet Pro 100] (rev 08)	e100.o	1	9
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	SCSI storage controller: Adaptec 7892A (rev 02)	aic7xxx.o	1	10
<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Ethernet controller: 3Com Corporation 3c905C-TX [Fast Etherlink] (rev 78)	3c90x.o	1	12

- Confirm that the defaults in the Basic Information section are appropriate for your server.

If you change the name of the configuration, use a name no longer than 15 characters.

**Note:** If you have more than 895MB of RAM installed on your server, the available memory is not reported accurately at this stage. The correct amount of memory is reported after you reboot the server.

The default amount of memory reserved for the console operating system — 128MB — is sufficient for managing up to three or four virtual machines.

Increase this to 192MB for eight virtual machines, 272MB for 16 virtual machines, 384MB for 32 virtual machines or 512MB for more than 32 virtual machines. For background, see [Sizing Memory on the Server on page 249](#).

**Note:** Certain storage controllers are sensitive to the memory size setting. If your server uses a PercRAID or MegaRAID controller, do not use a memory size in the range 241–271.

6. Allocate storage and network adapters to be used by the console operating system and virtual machines on the server. Be sure that both the console operating system and the virtual machines have access to at least one device in each category.

**Storage:** A SCSI or RAID adapter should be shared if you want to use that adapter or array for both the console operating system and virtual machines.

When you are allocating SCSI or RAID devices, the unit of device allocation is a PCI card device. You may connect multiple SCSI or RAID disks, CD-ROM drives, tape drives and other devices to the SCSI or RAID adapter.

You should give as many SCSI or RAID devices to the virtual machines as possible to ensure that the majority of your mass storage resources are used by your virtual machines. If you do not have any IDE disks, you may have to allocate at least one SCSI or RAID device to the console operating system, since the console operating system needs to have a disk from which it and the VMkernel can boot.

**Note:** If you are installing ESX Server on a Dell PowerEdge 8450, you must assign the on-board Symbios controller for use exclusively by the virtual machines.

Some adapter cards have multiple functions, which means there are multiple adapters on each card. When you allocate a SCSI or RAID device to the console operating system or to the VMkernel, you are effectively allocating all the SCSI or RAID disks, CD-ROM drives and other attached devices along with the adapter. As a result, you have only coarse-grained control over how you allocate SCSI and RAID devices.

Consider this example: Suppose your machine has SCSI adapters `vmhba0` and `vmhba1` that are on the same SCSI adapter card. If you choose to share one of the adapters, you must share both. Similarly, if you choose to allocate one of the adapters for use by virtual machines, you must allocate both for use by virtual machines.

**Network:** It is generally best to assign the first Ethernet adapter on the list to the console operating system and set the other adapters to be used by virtual

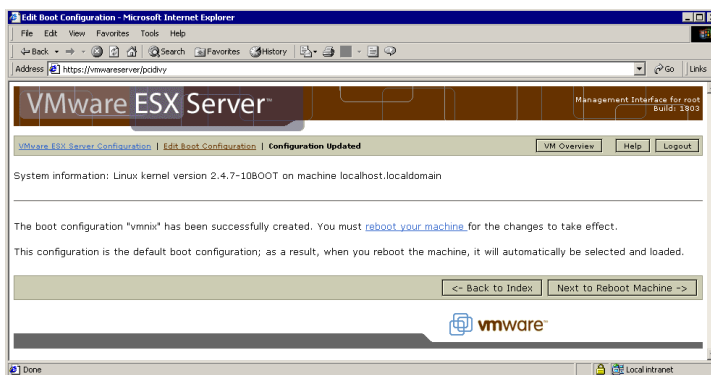
machines. If you assign the first adapter to be used by virtual machines, the console operating system may try to use an inappropriate driver for its network adapter. Ethernet adapters cannot be shared between the console operating system and virtual machines at this stage. To configure a shared adapter later, see [Sharing Network Adapters and Virtual Networks on page 224](#).

As with SCSI and RAID controllers, the unit of device allocation is a PCI card. Some network adapter cards are multifunction PCI cards, which means there are multiple adapters on each card. Only one network adapter is displayed in the list of devices. When you allocate that device to the console operating system or to the VMkernel, you are effectively allocating all the adapters on that card.

It is generally good to give as many network adapters to the virtual machines as possible. Doing so helps ensure that the majority of your network resources are devoted to the virtual machines. Because the console operating system is intended primarily as a management interface, you should minimize resources allocated to the console operating system. You need to allocate at least one Ethernet device to the console operating system in order to manage your ESX Server machine remotely.

In the likely event that you have fewer Ethernet devices than virtual machines, you can share VMkernel Ethernet adapters among the virtual machines with little performance penalty.

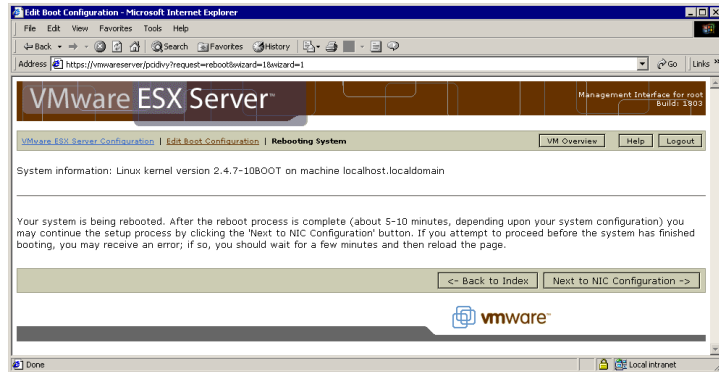
7. Click **Save Configuration**.



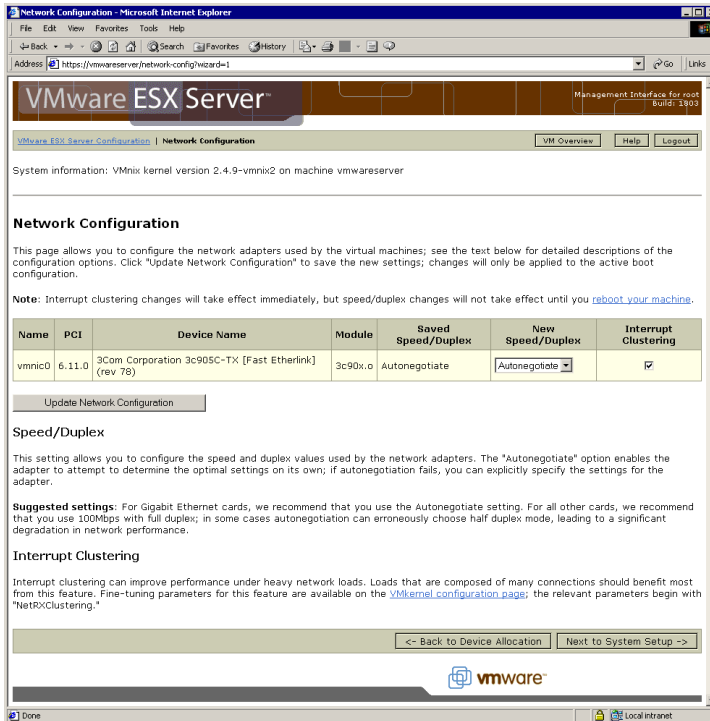
8. A confirmation screen lets you know the boot configuration is complete.

Click **Next to Reboot Machine** to restart your server using the configuration you just set up.

## Installing, Configuring and Upgrading ESX Server



9. After the server has rebooted, click **Next to NIC Configuration** to configure speed and duplex settings for the network adapters assigned for use by virtual machines.



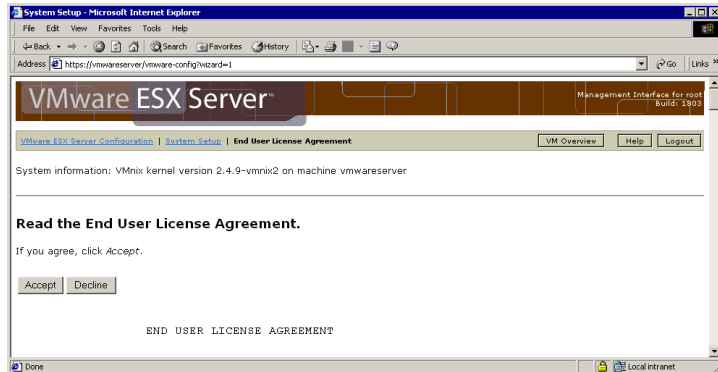
10. The default setting for the network adapters is 100Mbps, full duplex. Accept the default or choose a different setting from the drop-down list.

If your virtual machines have heavy network loads composed of many connections, you may be able to improve performance by enabling interrupt clustering. For details, see [Performance Tuning for Heavy Network Loads on page 228](#).

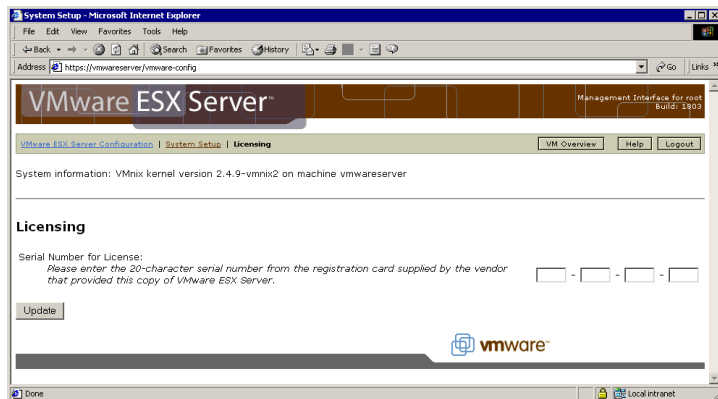
Click **Update Network Configuration**.

11. Click **Next to System Setup**.

## Installing, Configuring and Upgrading ESX Server



12. Read the ESX Server license agreement, then click **Accept** to accept it.

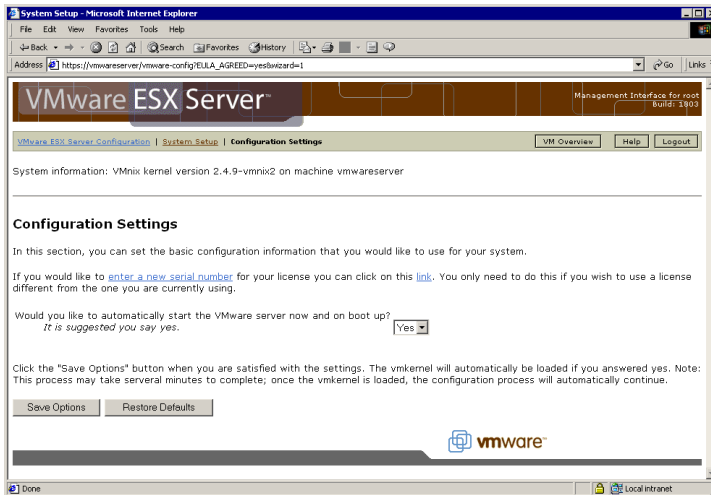


13. Enter your serial number, then click **Update**.

14. A registration screen provides information on registering ESX Server. When you have finished with this screen, click **Continue**.

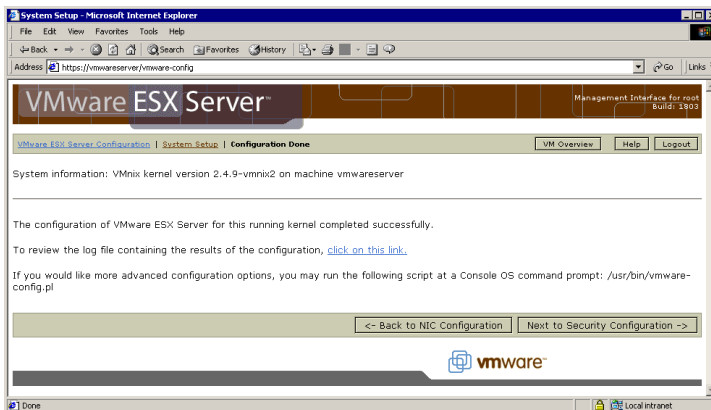


## Installing, Configuring and Upgrading ESX Server

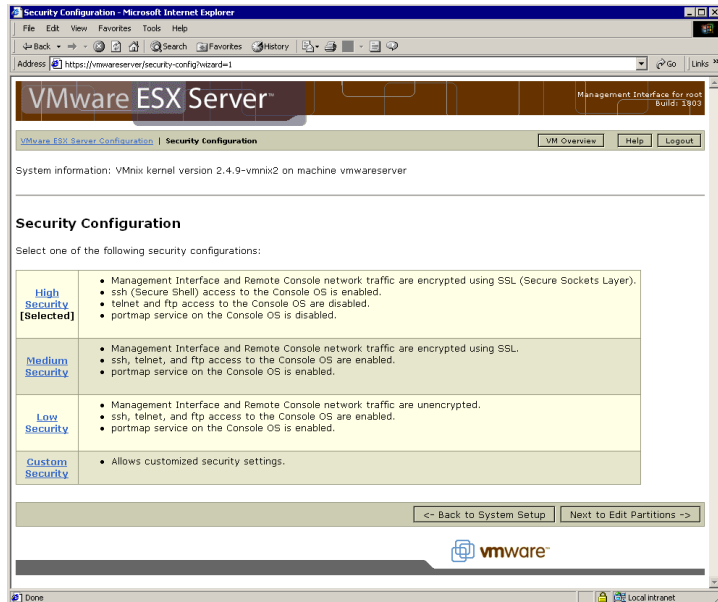


15. If necessary, change the server start-up setting. In most cases, the defaults are appropriate.

Click **Save Options**.



16. A confirmation screen notifies you that you have completed the basic configuration of the kernel. Click **Next to Security Configuration**.



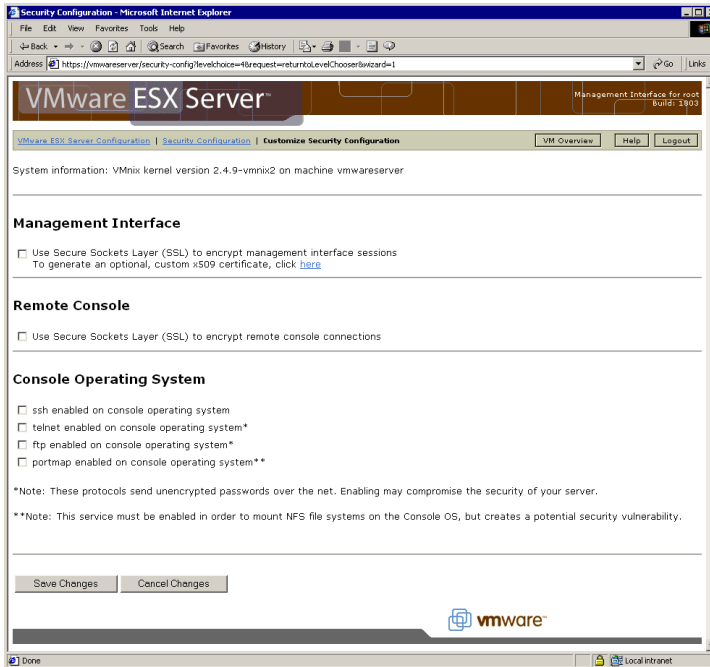
17. Select the security level for the VMware ESX Server machine and the network traffic generated by VMware ESX Server.

When you configure a more secure machine, you have fewer options for connecting to it, as less secure methods for connecting to the computer (such as Telnet or FTP) are disabled.

High Security is selected by default. If this is appropriate, click **Next to Edit Partitions**.

To change to a different standard security setting, click the setting you want to use.

To select custom settings, click **Custom Security**.



The Custom Security Configuration page lets you customize your settings for encrypting remote console and VMware Management Interface connections using the Secure Sockets Layer protocol. VMware ESX Server uses OpenSSL. See [Appendix B: The OpenSSL Toolkit License on page 279](#) for more information.

You may also enable SSH, Telnet, FTP and portmap (needed for NFS) on the console operating system.

After you make your selections, click **Save Changes**. Or if you want to generate a custom certificate for use with SSL, click the word **here** in the Management Interface section.

## Installing, Configuring and Upgrading ESX Server

Security Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://vmwareserver/security-config/request=editcertificate&wizard=1>

VMware ESX Server Management Interface for root Build: 1903

VMware ESX Server Configuration | Security Configuration | **Edit SSL Certificate** VM Overview Help Logout

System information: VMnix kernel version 2.4.9-vmnix2 on machine vmwareserver

In order to function properly, SSL requires a certificate containing information about the location and owner of a server. All of this data is optional, but recommended. Displayed below are the contents of the current certificate.

Number of days before certificate expires	365
State or Province	Other or Unknown
Server's hostname	vmwareserver
City	
Department Name	
Two letter country code	United States of America (US)
Administrator's email address	
Company/Organization Name	

Save Changes Cancel Changes

vmware

Done Local intranet

Enter the information you want to include in your security certificate, then click **Save Changes**.

You are finished with the basic configuration of your server.

Next, you need to edit the partitions on the drive or drives used to store virtual machines.

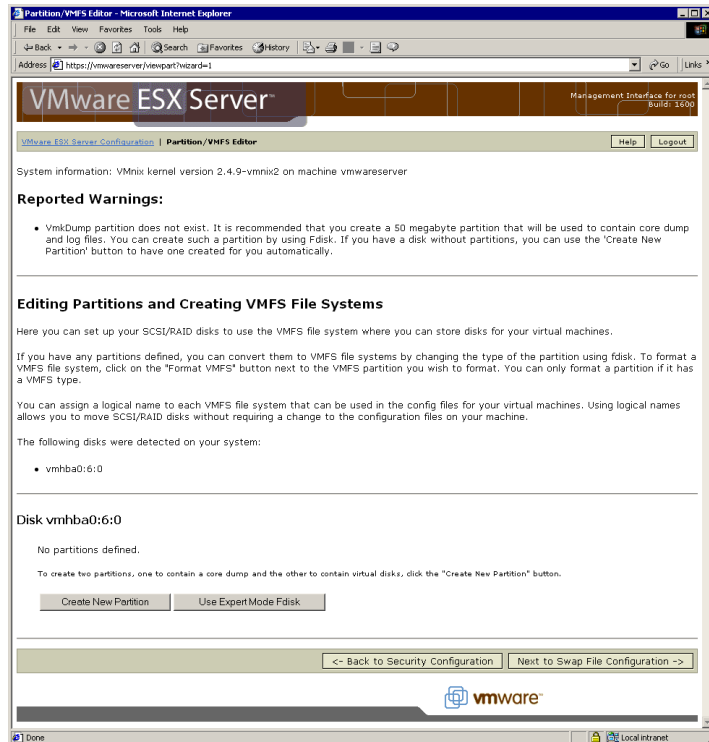
### Configuring Storage for Virtual Machine Files

Details of the next steps in configuring your server depend on whether the storage device you use to store virtual machines is used only for storing virtual machines or is shared between virtual machines and the console operating system. Jump to the appropriate section for your configuration.

- [Using an Entire SCSI Disk or RAID Array for Virtual Machines on page 46](#)
- [Sharing a SCSI Drive or RAID Array with the Console Operating System on page 51](#)

### Using an Entire SCSI Disk or RAID Array for Virtual Machines

If you have a SCSI disk or RAID array in addition to the disk or array that holds the console operating system, you see the following screen. If you have only one SCSI disk or RAID array, skip this section and see [Sharing a SCSI Drive or RAID Array with the Console Operating System on page 51](#). For background on how SCSI devices are identified, see [Determining SCSI Target IDs on page 208](#).



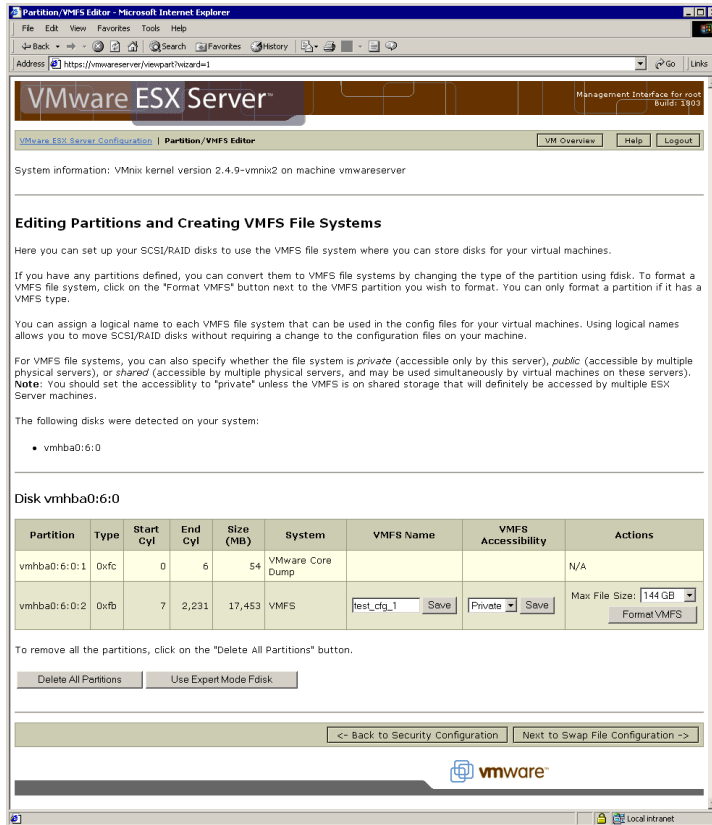
1. Set up partitions for your virtual machines.

In this example, you want to make all of disk `vmhba0 : 6 : 0` available to store virtual machine files.

Click **Create New Partition** to create a small core dump partition and a VMFS (VMware ESX Server file system) partition that uses the rest of the space available on the disk or array.

The VMFS partition provides high-performance access to the virtual machine's files — essentially the same performance you would get if the virtual machine were installed on a raw SCSI partition.

The core dump partition stores information generated if the VMkernel crashes. The core dump information is important in debugging any problems with the VMkernel.



- You see a screen that reports the sizes of the two partitions you have just created.

You should assign a logical name to the VMFS partition. Choose a name that makes it easy to identify this particular partition even if you later decide to move

the device to a different machine. Enter the logical name in the field under VMFS Name and click Save.

In the VMFS Accessibility field, choose **Private**, **Public** or **Shared**, then click **Save**.

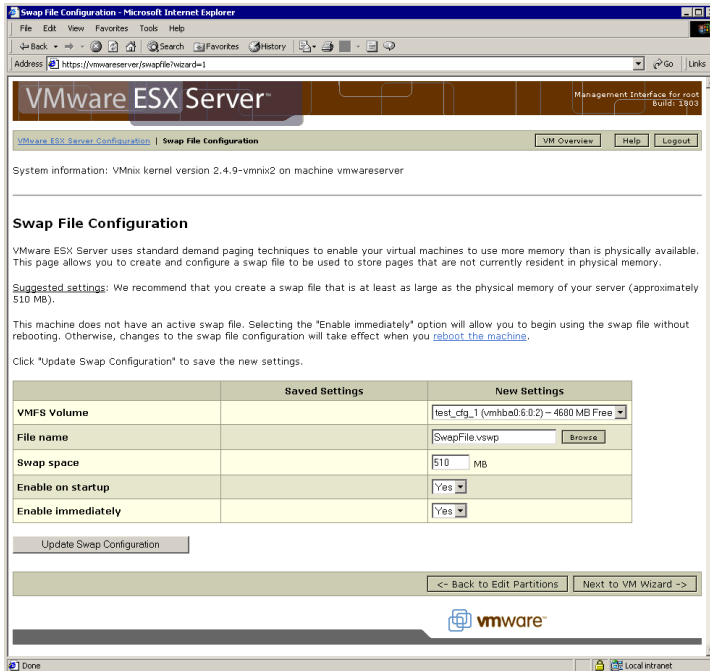
By default, VMFS accessibility is set to Private. If the VMFS partition is available to multiple physical servers (because it is on a storage area network that can be accessed by multiple servers), you should change this setting — typically to **Public**. Choosing **Public** makes the VMFS partition available to multiple physical servers and to virtual machines on those servers, but only to a single server at a time. Choose **Shared** to make the VMFS partition available to virtual machines on multiple physical servers at the same time. The **Shared** option is useful for failover-based clustering among virtual machines on multiple servers. For background, see [Using Storage Area Networks with ESX Server on page 212](#).

If you plan to create virtual machines with virtual disks larger than the default maximum size of 144GB, change the value in the **Max File Size** field.

Click **Format VMFS** to format the partition.

Click **Next to Swap File Configuration** to set up the swap space that ESX Server uses as part of its memory management features. For background, see [Memory Resource Management on page 239](#).



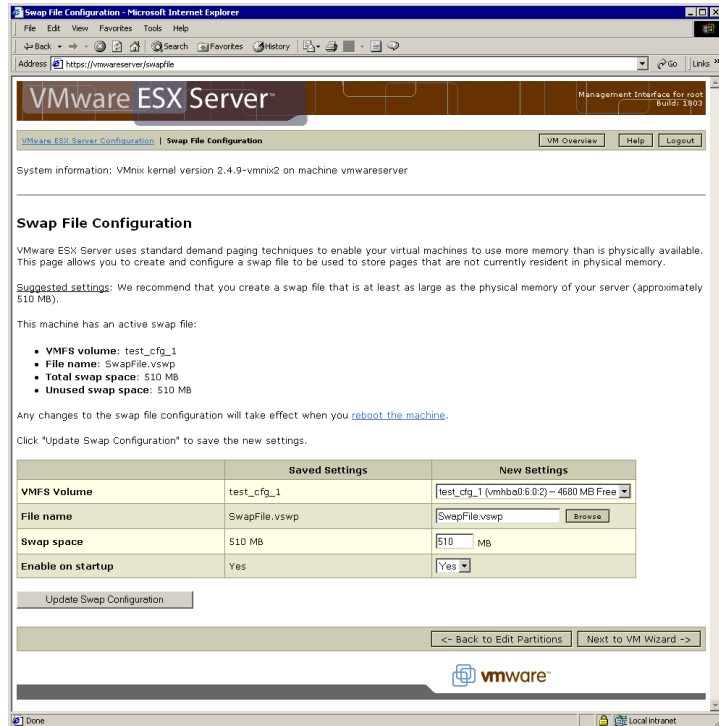


3. Accept the defaults or make any needed changes to the swap file configuration. The default configuration creates a swap file equal to the total amount of memory on the server.

Click **Update Swap Configuration**.

**Note:** If you make changes to the amount of swap space after this initial configuration, you must restart the server before they will take effect.

4. The page refreshes, showing the new configuration settings.

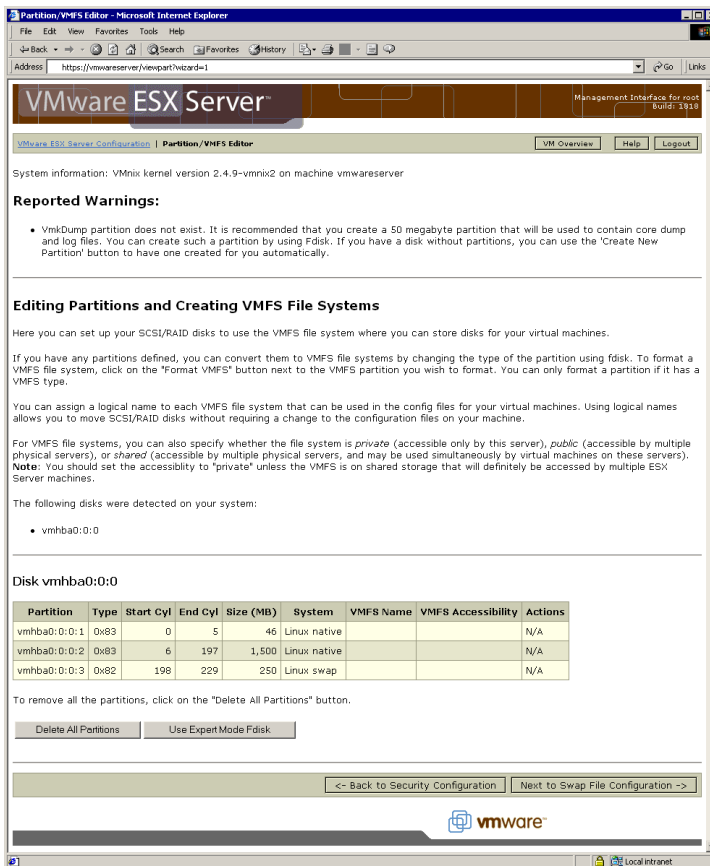


Click **Next to VM Wizard** to begin creating a virtual machine. The Setup Wizard logs you out and suggests that you log in as an ordinary user before creating a virtual machine.

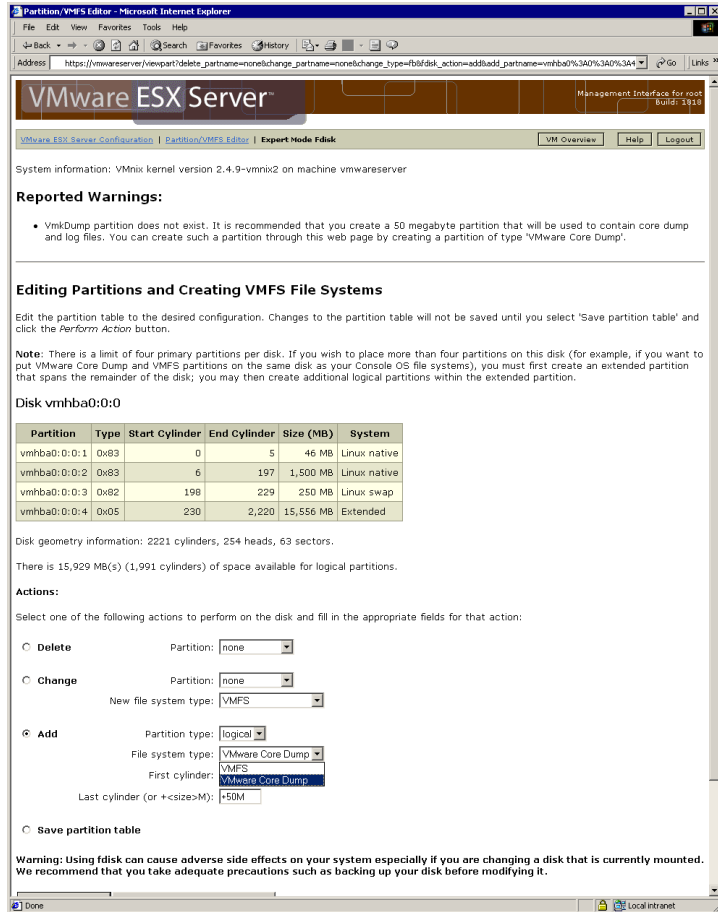
See [Creating a New Virtual Machine on page 59](#) for instructions on creating and configuring a virtual machine.

## Sharing a SCSI Drive or RAID Array with the Console Operating System

In this example, the disk `vmhba0 : 0 : 0` already contains the partitions used by the console operating system. You should not make changes to these partitions. For background on how SCSI devices are identified, see [Determining SCSI Target IDs on page 208](#).



1. Click Use Expert Mode Fdisk.



2. First add a small core dump partition. The core dump partition stores information generated if the VMkernel crashes. The core dump information is important in debugging any problems with the VMkernel.

Select **Add**, use the default of **logical** and choose **VMware Core Dump** from the list of file system types. In this scenario, an extended partition, to contain this logical partition, should already exist. If it doesn't, you must add an extended partition before you add the logical partition.

Do not change the number in the **From cylinder** field.

Change the number in the **Last cylinder** field to +50M (be sure to include the + sign) to set aside about 50MB for the core dump partition. The partition is at least 50MB, but is likely to be somewhat larger because partitions must begin and end on cylinder boundaries.

3. Click **Perform Action**.

**Note:** No changes are actually written to disk until you select **Save Partition Info**, then click **Perform Action**.

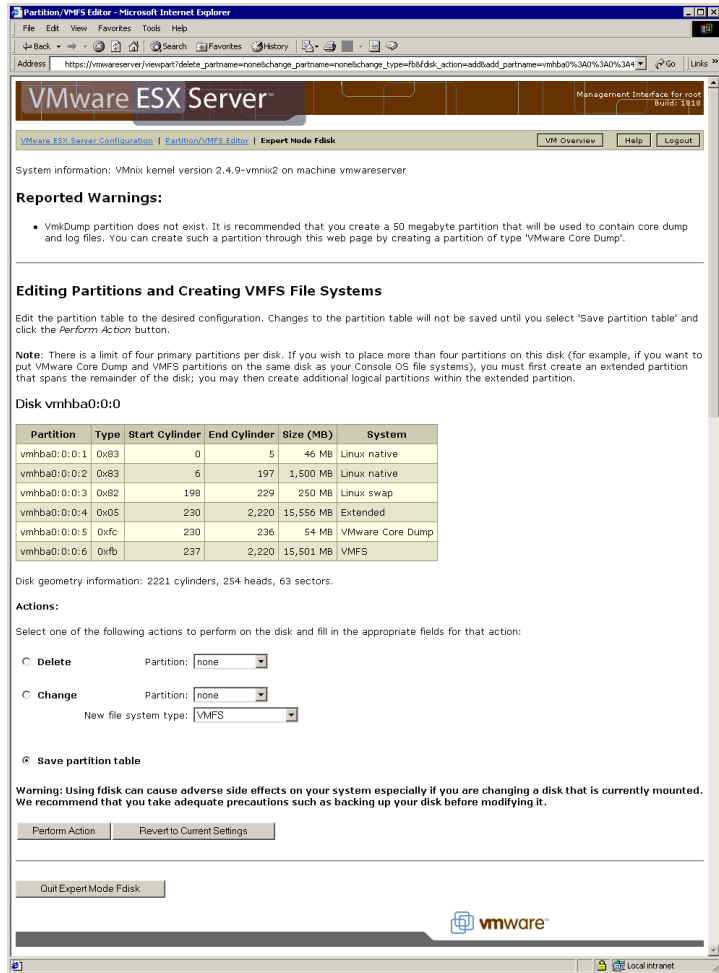
4. Use the rest of the disk or array as a VMFS partition, where you store virtual machine disk files.

The VMFS partition provides high-performance access to the virtual machine's files — essentially the same performance you would get if the virtual machine were installed on a raw SCSI partition.

Select **Add**. You may use the default of **logical** or change the setting to **primary** and choose **VMFS** from the list of file system types. Keep in mind that only four primary partitions can exist on a drive. If you have an extended partition (to contain logical partitions), that counts as one of your four primary partitions.

Do not change the numbers in the **From cylinder** and **Last cylinder** fields.

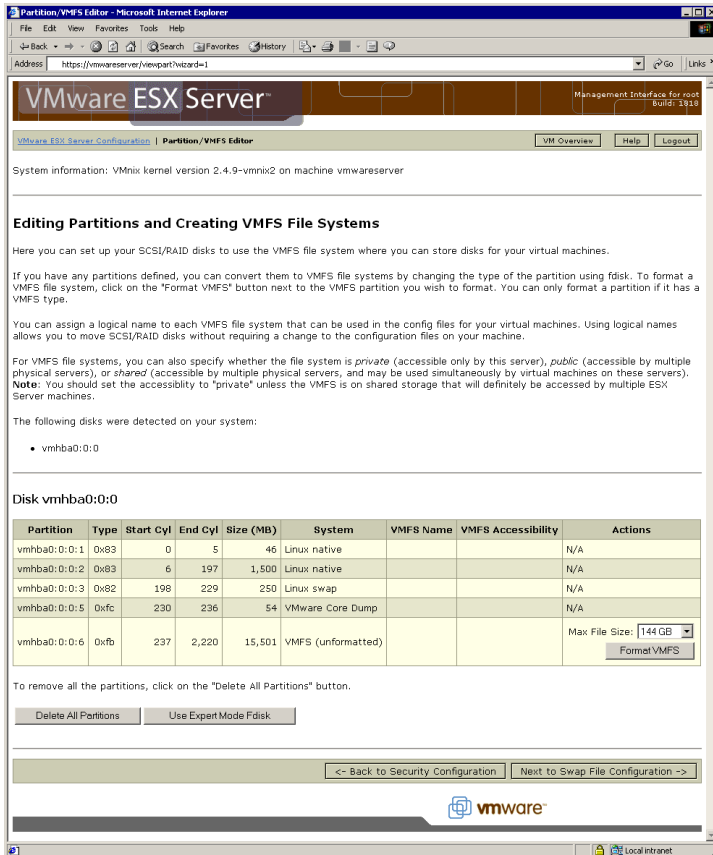
5. Click **Perform Action**.



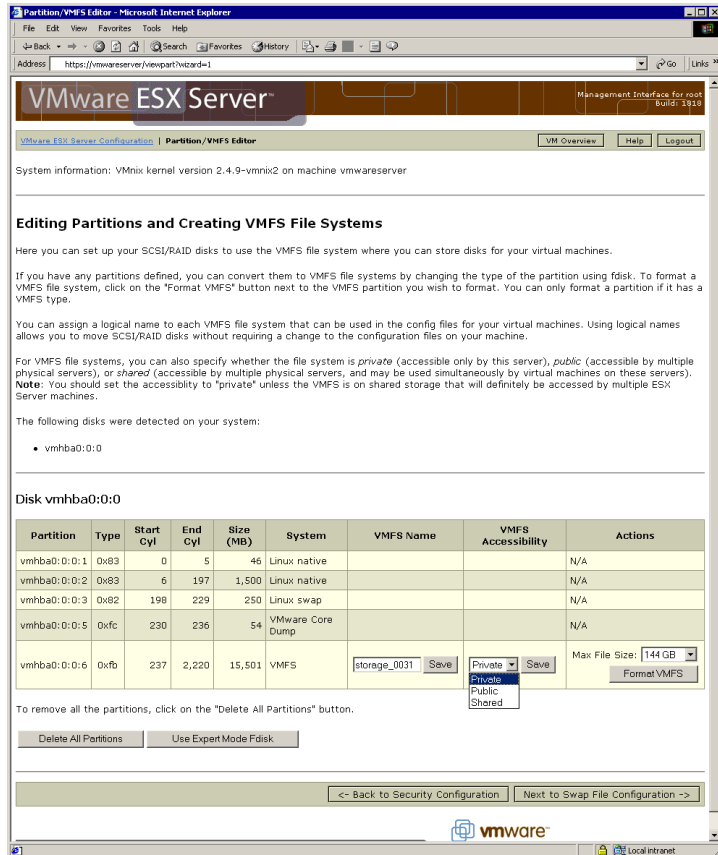
6. Select **Save partition table**.

7. Click **Perform Action**.

**Note:** At this point, your changes are committed to the disk or array.



8. Locate the table row with information about the VMware partition you just created. Click the **Format VMFS** button in that row.



- You should assign a logical name to the VMFS partition. Choose a name that makes it easy to identify this particular disk even if you later decide to move the device to a different machine. Enter the logical name in the field under VMFS Name and click **Save**.

In the VMFS Accessibility field, choose **Private**, **Public** or **Shared**, then click **Save**.

By default, VMFS accessibility is set to Private. If the VMFS partition is available to multiple physical servers (because it is on a storage area network that can be accessed by multiple servers), you should change this setting — typically to **Public**. Choosing **Public** makes the VMFS partition available to multiple physical servers and to virtual machines on those servers, but only to a single server at a



time. Choose **Shared** to make the VMFS partition available to virtual machines on multiple physical servers at the same time. The **Shared** option is useful for failover-based clustering among virtual machines on multiple servers. For background, see [Using Storage Area Networks with ESX Server on page 212](#).

Click **Next to Swap File Configuration** to set up the swap space that ESX Server uses as part of its memory management features. For background, see [Memory Resource Management on page 239](#).

System information: VMnix kernel version 2.4.9-vmnix2 on machine vmwareserver

### Swap File Configuration

VMware ESX Server uses standard demand paging techniques to enable your virtual machines to use more memory than is physically available. This page allows you to create and configure a swap file to be used to store pages that are not currently resident in physical memory.

**Suggested settings:** We recommend that you create a swap file that is at least as large as the physical memory of your server (approximately 2047 MB).

This machine does not have an active swap file. Selecting the "Enable immediately" option will allow you to begin using the swap file without rebooting. Otherwise, changes to the swap file configuration will take effect when you [reboot the machine](#).

Click "Update Swap Configuration" to save the new settings.

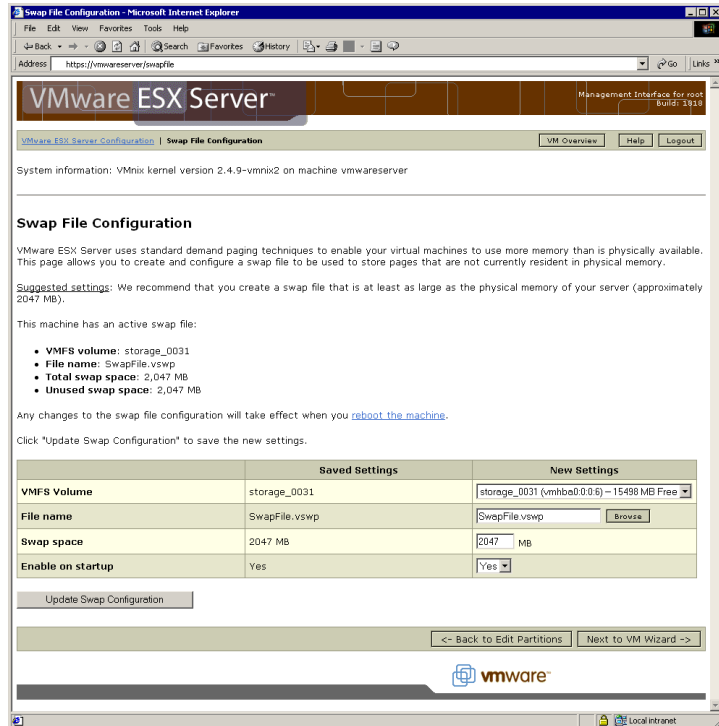
	Saved Settings	New Settings
VMFS Volume		storage_0031 (vmhba0:0:0:0) - 15498 MB Free
File name		SwapFile.vswp <input type="button" value="Browse"/>
Swap space		2047 MB
Enable on startup		Yes
Enable immediately		Yes

- Accept the defaults or make any needed changes to the swap file configuration. The default configuration creates a swap file equal to the total amount of memory on the server.

Click **Update Swap Configuration**.

**Note:** If you make changes to the amount of swap space after this initial configuration, you must restart the server before they will take effect.

11. The page refreshes, showing the new configuration settings.



Click **Next to VM Wizard** to begin creating a virtual machine. The Setup Wizard logs you out and suggests that you log in as an ordinary user before creating a virtual machine.

See [Creating a New Virtual Machine on page 59](#) for instructions on creating and configuring a virtual machine.

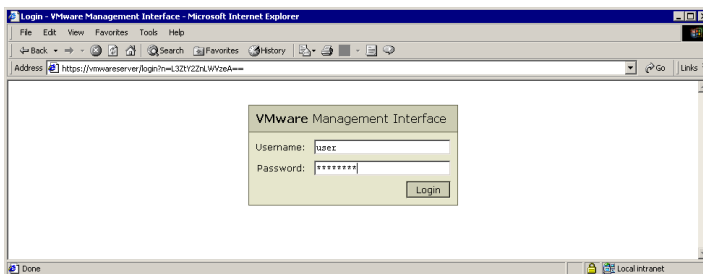
## Creating a New Virtual Machine

The Virtual Machine Wizard guides you through the basic steps needed to create a virtual machine on your server. Any user who has an account on the server's console operating system may log in to the wizard and create a virtual machine. If you are logged in as root, you may wish to log out at this point, then log in again as a user authorized to manage the new virtual machine.

To return to the wizard later, use this URL:

`http://<hostname>/vmcfg-esx`

If you are logged into the VMware Management Interface, on the Overview page, click **Create VM** to create a new virtual machine.



1. Enter your user name and password, then click **Login** to begin using the wizard.

**ESX VM Configuration: VMware Management Interface - Microsoft Internet Explorer**

Address: <https://vmwareserver/vmcf/ess>

**Create VM | VMware Management Interface for user**

VMs on vmwareserver | **New VM** [Help] [Logout]

**New VM**

**Basic Settings**

Operating System:

Display Name:

Virtual Machine Filename:

Memory Size (RAM):  MB (Maximum new VM size: 812 MB)

**SCSI Disk**

scsi0:1

VMFS Volume:

Enter a unique name for this disk:

Disk Size:  MB

Disk Mode:

**Networking**

Ethernet Adapter 0:

☒ Use vmmic0 ☐ Use vmxnet ☐ Use vmxnet2

**vmmic0:** Bind this virtual NIC to a physical NIC on the server.  
**vmxnet:** Bind this virtual NIC to a virtual switch that connects to other virtual machines (and optionally to the console OS).  
**vmxnet2:** May offer better performance, especially for gigabit Ethernet and network-intensive workloads.  
**vmmic0:** Good for most other uses, compatible with drivers available in most guests.

**CD-ROM Drive**

Enter the full path and filename of the device or CD image file you wish to use. You can click "View Console File System..." to see what devices and files are available.

CD-ROM Present: ☒ Yes ☐ No

Filename:

☐ File is an ISO image

☒ Start Connected

**Floppy Drive**

Enter the full path and filename of the device or CD image file you wish to use. You can click "View Console File System..." to see what devices and files are available.

Floppy Present: ☒ Yes ☐ No

Filename:

☐ File is a floppy image

☐ Start Connected

**Misc**

Remote Display Depth:

Suspend Location: ☒ Configuration file directory ☐ VMFS Volume:  ☐ Other location:

Storing suspended state files on a VMFS volume will significantly improve the speed of suspend and resume operations.

Use Debug Monitor:

[Undo Changes] [Save Changes]

2. Choose the guest operating system for your virtual machine. Corresponding default entries appear for other configuration settings.
3. Make any changes you wish to the default settings.

**Basic settings:** The name you enter in the **Display Name** field is the name that is listed in the VMware Management Interface. Be sure to enter a name that

allows you to distinguish this virtual machine from others you have created or plan to create.

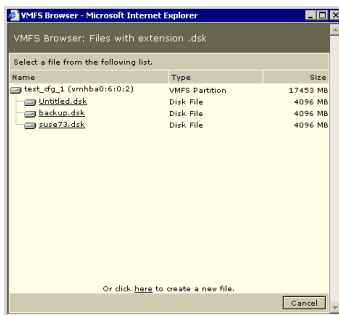
Be sure that the entry in the **Virtual Machine Filename** field is unique. The default path and filename are based on the guest operating system you have chosen. If other virtual machines have been created on this server, you must change the path to create a new, unique directory for the new virtual machine.

The default **Memory Size** setting depends on the guest operating system you have selected. You may need to change it to meet the demands of applications you plan to run in the virtual machine. You may change this setting later, using the Configure VM page of the VMware Management Interface.

For background on allocating memory to virtual machines, see [Sizing Memory on the Server on page 249](#).

**SCSI disk:** Be sure that the virtual machine's file name is unique. The filename should end in `.disk`.

Click the **Browse** button in the SCSI Disk section if you want to view file names already in use or if you want to use an existing virtual disk file with this virtual machine.



Click the name of a file in the browser window to select it.

Select the disk mode for your virtual disk. ESX Server can use disks in four different modes: persistent, nonpersistent, undoable and append.

- **Persistent:** Disks in persistent mode behave exactly like conventional disk drives on a computer. All writes to a persistent disk are written out permanently to the disk as soon as the guest operating system writes the data.

- **Nonpersistent:** All changes to a disk in nonpersistent mode are discarded when a virtual machine session is powered down.
- **Undoable:** When you use undoable mode, you have the option later of keeping or discarding changes you have made during a working session. Until you decide, the changes are saved in a redo-log file.
- **Append:** Append mode also stores changes in a redo log. It continually adds changes to the redo log until you remove the redo-log file or commit the changes using the `commit` command in `vmkfstools` (see [Using vmkfstools on page 199](#)).

The setup process allows you to create one virtual disk for your virtual machine. You can add more virtual disks later, using the Configure VM page of the VMware Management Interface.

**Networking:** Select the way you want to connect this virtual machine to the network. You can select a vmnic adapter, which connects the virtual machine to the physical network adapter, allowing the virtual machine to look and act as another computer on the network. Or you can connect the virtual machine to an internal network of other virtual machines by selecting a vmnet adapter. All the virtual machines on this computer connected to a particular vmnet are on the same network.

Also, you need to select the network driver for this network connection. You can choose between the vlane driver, which installs automatically, and the vmxnet driver, which provides better network performance. The difference in network performance is most noticeable if the virtual machine is connected to a Gigabit Ethernet card.

If you choose vmxnet, you must configure the driver manually when you install VMware Tools in the guest operating system (see [Installing a Guest Operating System and VMware Tools on page 70](#)).

**Note:** If you use vmxnet in a Linux virtual machine, the virtual network device will not be visible to the guest operating system until you install VMware Tools (see [Installing VMware Tools and the Network Driver in a Linux Guest on page 76](#)). After you install VMware Tools, run `netconfig` or another network configuration utility in the virtual machine to set up the virtual network adapter.

After the virtual machine is created, you can use the Configure VM page to assign additional network adapters to the virtual machine.

If you need help determining which network adapter is associated with a particular device name, you can use the console operating system's `findnic` command (see [The VMkernel Network Card Locator on page 220](#)).

**CD-ROM drive and floppy drive:** If your server contains a CD-ROM drive or floppy drive, specify the path to the drive in the `/dev` directory and whether you want the virtual machine to connect to this device when the virtual machine powers on. A device can be connected to only one virtual machine on a server at a time.

You may also choose to point the CD-ROM drive to an ISO disc image file and the floppy drive to a floppy disk image file. To do so, type the path to the image file in the appropriate **Filename** entry field and select **File is an ISO image**.

**Misc.:** If you want, you can change the color depth of your display using the **Remote Display Depth** setting. A higher color depth setting slows down screen redraws and increases network load when you use a remote console to view a virtual machine across a network connection. However, with greater color depth, you get better color resolution and fidelity. The default setting is 8. Other options are 15, 16 or 24.

When you suspend a virtual machine, a suspended state file is created. By default, it is saved in the virtual machine's directory — the directory shown in the **Virtual Machine Filename** field.

You may want to select a different location for better performance or to avoid running out of space on the partition that holds the virtual machine directories.

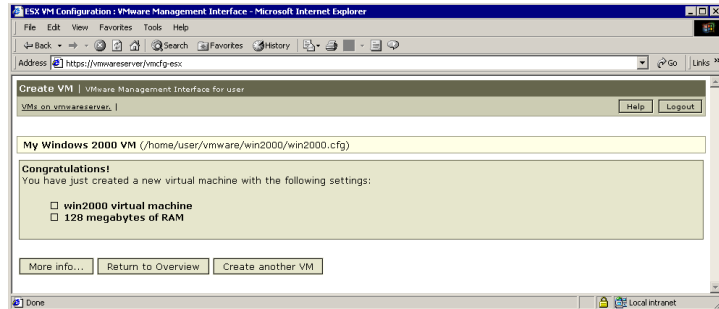
For fastest suspend and restore operations, select **VMFS Volume** and choose the appropriate VMFS volume from the drop-down list. ESX Server automatically adds a suffix to the name of the suspended state file to ensure that one virtual machine does not overwrite the suspended state file of another.

If you want to save the suspend file in a different directory, specify the path in the **Other location** entry field.

Set the Use Debug Monitor option to **No** unless you are working with VMware support to debug a specific issue.

If you want to reset the entries to the defaults, click **Undo Changes**.

4. When you are satisfied with the settings, click **Create VM**.



5. The confirmation page includes information on some basic configuration settings for your new virtual machine.
6. To create an additional virtual machine, click **Create another VM**. To go to the main page of the management interface, click **Return to Overview**.



# Installing, Configuring and Upgrading ESX Server

VMware ESX Server

Management Interface for user  
Build: 1803

VMS on vmwareserver.

Virtual Machine	Rights	%HB	Up Time	% CPU	% RAM
My Windows 2000 VM	r w x	0	0d 0h 0m	0	0
My Linux VM	r w x	0	0d 0h 0m	0	0
My Windows NT4 VM	r w x	0	0d 0h 0m	0	0
System Summary:			0d 0h 33m	3	26

Create VM

Last Updated: 04/13/2002 15:31:30

Refresh

### Installing the VMware Remote Console

#### Installing a Console in a Windows NT 4.0 or Windows 2000 Host

Download the installer:

- [VMware-console-1.5.0-1803.exe](#)

To install the remote console, double-click VMware-console-1.5.0-1803.exe and follow the instructions in the installation wizard.

#### Installing a Console in a Linux Host

Download the installer appropriate for your Linux distribution:

- [VMware-console-1.5.0-1803.i386.rpm](#)
- [VMware-console-1.5.0-1803.tar.gz](#)

In a terminal window, become root (su) so you can carry out the initial installation steps. Then do one of the following:

- If you downloaded the RPM installation package, run the RPM file:
  - `rpm -Uvh VMware-console-1.5.0-1803.i386.rpm`
- If you downloaded the tar installation archive, unpack it and run the installer:
  - `tar xzf VMware-console-1.5.0-1803.tar.gz`
  - `cd vmware-console-distrib`
  - `./vmware-install.pl`

#### Configuring MIME-type support for Netscape Navigator

Please see [Setting a MIME Type to Launch the Remote Console in Netscape](#) for full documentation.

#### Column Descriptions

##### Virtual Machine

This column contains each virtual machine's display name as specified in its configuration file. If a virtual machine's configuration file does not specify a display name, then the path to the

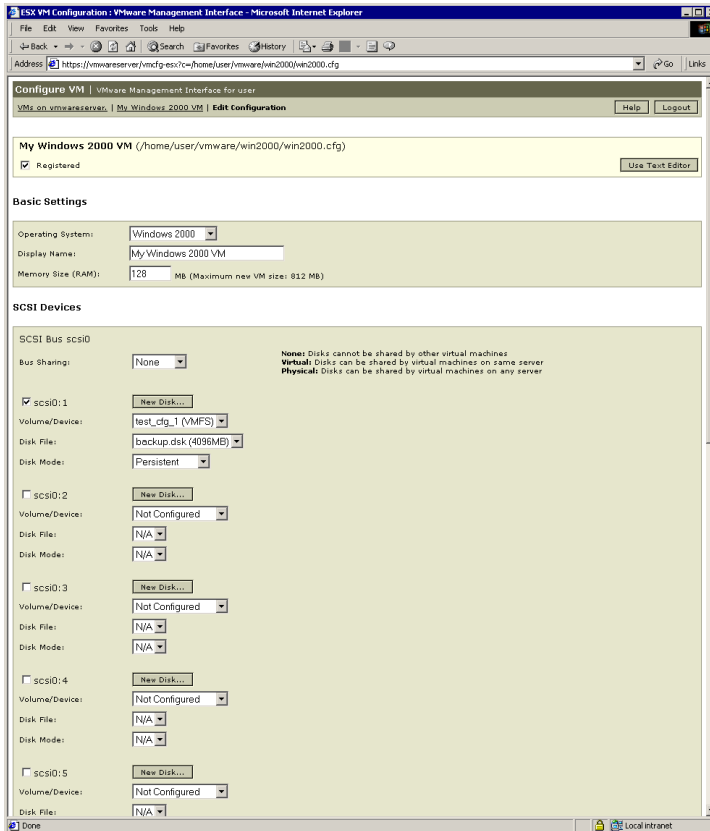
#### Legend

- Virtual Machine Menu**  
Mouse over this icon to open a menu of control options for the corresponding virtual machine.
- Power-Off Controls**  
From top to bottom: Controls indicating that the corresponding virtual machine is powered off; can be powered off gracefully and cannot be powered off gracefully.
- Suspend Controls**  
From top to bottom: Controls indicating that the corresponding virtual machine is suspended; can be suspended and cannot be suspended.
- Power-On Controls**  
From top to bottom: Controls indicating that the corresponding virtual machine is powered on; can be powered on and cannot be powered on.
- Reset Controls**  
From top to bottom: Controls indicating that the corresponding virtual machine can be rebooted gracefully and cannot be rebooted gracefully.

- To see additional details about a virtual machine, click the virtual machine's name.



8. To change settings for your virtual machine, be sure the virtual machine is powered off, then click **Edit VM Configuration**. The Configure VM page appears.



Top section of page for editing a virtual machine configuration

The **Registered** check box at the top of the page controls whether the virtual machine is listed on the overview page of the management interface. Check the box to include the virtual machine in the list. Remove the check to remove the virtual machine from the list.

**Note:** Virtual machines appear in the list only if their configuration files are stored locally on the ESX Server computer. If the configuration files are stored on an NFS-mounted drive, the virtual machines are not listed.

## Installing, Configuring and Upgrading ESX Server

ESX VM Configuration: VMware Management Interface - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address: <https://vmwareserver/vmcf?ess?c=/home/user/vmware/vm2000/vm2000.cfg>

Disk Mode: N/A

☐ SCSI ID: 6 [New Disk...](#)

Volume/Device: Not Configured

Disk File: N/A

Disk Mode: N/A

### Networking

Ethernet Adapter 0: vmnic0 vmnic: Bind this virtual NIC to a physical NIC on the server.  
vmxnet: Bind this virtual NIC to a virtual switch that connects to other virtual machines (and optionally to the Console OS).  
vmxnet3: May offer better performance, especially for Gigabit Ethernet and network-intensive workloads.  
vance: Good for most other uses, compatible with drivers available in most guests.

☒ Use vance ☐ Use vmxnet

Ethernet Adapter 1: Not Installed ☒ Use vance ☐ Use vmxnet

Ethernet Adapter 2: Not Installed ☒ Use vance ☐ Use vmxnet

### CD-ROM Drive

Enter the full path and filename of the device or CD image file you wish to use. You can click "View Console File System..." to see what devices and files are available.

CD-ROM Present: ☒ Yes ☐ No

Filename: /dev/cdrom [View Console File System...](#)

☐ File is an ISO image

☒ Start Connected

### Floppy Drive

Enter the full path and filename of the device or CD image file you wish to use. You can click "View Console File System..." to see what devices and files are available.

Floppy Present: ☒ Yes ☐ No

Filename: /dev/fd0 [View Console File System...](#)

☐ File is a floppy image

☐ Start Connected

### Misc

Remote Display Depth: 8

Suspend Location: ☒ Configuration file directory Storing suspended state files on a VMFS volume will significantly improve the speed of suspend and resume operations.

☐ VMFS Volume: vmfs (vmhba0:0:0:5 - 713 MB Free)

☐ Other location:

Use Debug Monitor: No

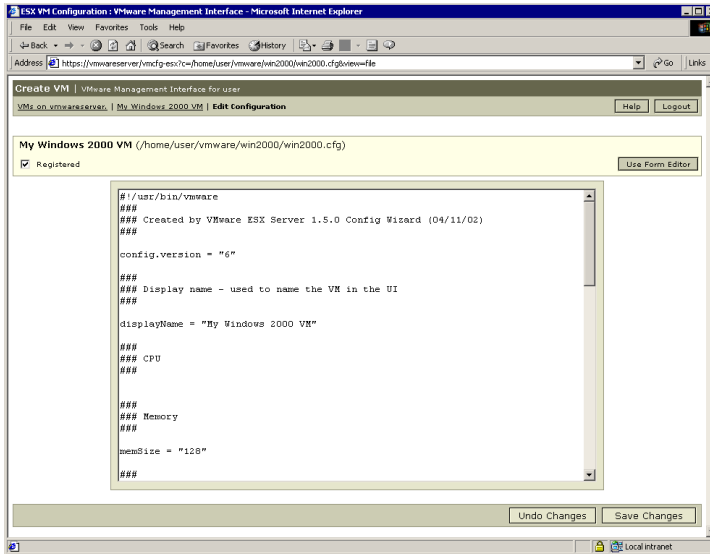
[Undo Changes](#) [Save Changes](#)

*Bottom section of page for editing a virtual machine configuration*

When you are finished, click **Apply Changes**.

You can edit the virtual machine configuration file itself remotely. On the Configure VM page, click **Use Text Editor**.

## Installing, Configuring and Upgrading ESX Server



For more information, see [Editing a Virtual Machine's Configuration Remotely](#) on page 99.

Your new virtual machine is like a new computer with a blank hard disk. You must install a guest operating system before you can use the virtual machine.

## Installing a Guest Operating System and VMware Tools

This section describes the following:

- [Installing a Guest Operating System in a Virtual Machine on page 70](#)
- [Migrating VMware Workstation and VMware GSX Server Virtual Machines on page 71](#)
- [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#)

In most cases, you configure your virtual machine with a blank (unformatted) SCSI virtual disk. You can install an operating system on this virtual disk just as you would on a new physical machine, using a standard installation CD-ROM and formatting the virtual disk at the appropriate place in the installation process.

You may also install from image files — ISO image files of installation CD-ROMs and floppy image files of any floppy disks needed for the installation. Use the VMware Management Interface to connect the virtual machine's drives to the appropriate image files before you begin the installation.

Another approach is to start with a virtual disk created with VMware Workstation 2.0 or higher or with VMware GSX Server, then configure the guest operating system to work with VMware ESX Server.

Once your guest operating system is installed, be sure to follow the directions below for installing VMware Tools and the network driver.

### Installing a Guest Operating System in a Virtual Machine

To install a guest operating system and other software, you should work on a separate workstation and use the VMware remote console. It is best not to run X on the server's console operating system.

For details on installing the remote console, see [Installing the Remote Console Software on page 81](#). Follow the directions in that section for starting a remote console on your Windows or Linux workstation and connecting to a virtual machine.

Insert the installation CD-ROM for your guest operating system in the server's CD-ROM drive. Click **Power On** on the remote console toolbar to begin setting up your guest operating system. See [Guest Operating Systems on page 149](#) for details on installing specific guest operating systems.

**Note:** When you are installing a guest operating system on a new virtual disk, you may see a message warning you that the disk is corrupted and asking if you want to place a partition table on the disk. This does not mean there is any problem with your physical hard disk. It simply means some data needs to be written to the file that holds your virtual hard disk. All you need to do is respond **Yes**. You also need to partition and format the virtual disk as you would with a new, blank hard drive.

### Migrating VMware Workstation and VMware GSX Server Virtual Machines

You can modify virtual machines created with VMware Workstation 2.0 or higher or VMware GSX Server to run on VMware ESX Server.

The virtual machine you want to migrate must be set up on a virtual SCSI disk. You then migrate it to run from a virtual SCSI disk under ESX Server.

Be sure you have enough space on the VMFS disk where you store virtual machines to hold the full size of the source virtual disk. In ESX Server the disk's full size is allocated at the time the virtual disk file is created. In VMware Workstation and GSX Server, the virtual disk file starts smaller and grows to the maximum size as data is added. Thus, a virtual disk defined as a 2GB disk may be contained in a 500MB file. When you migrate the virtual disk to ESX Server, it occupies 2GB of disk space.

When you install VMware Tools in the VMware ESX Server virtual machine, you may set up a new network driver. If you use the `vmxnet` driver, keep in mind that this driver is not suitable for a virtual machine running under VMware Workstation 2.x or under VMware GSX Server on a Linux host. If you think you may want to use this virtual machine under one of those products at a later time, you may find it convenient to do one of the following:

- Use the `v1ance` network driver.
- If you plan to use the `vmxnet` driver, make a copy of the virtual machine before you migrate it.

Follow these steps to migrate a virtual machine to VMware ESX Server.

1. Be sure you have access to the files in the directory that holds the source virtual machine. You may be able to mount the source location, or you may prefer to copy the files to a temporary folder on the console operating system.

If you are not sure where the source files are, open the virtual machine in the VMware product you used to create it, open the Configuration Editor (**Settings > Configuration Editor**). On a Windows host, click the name of the drive you want to migrate. In the Disk file section, click **Choose...** to see the location

information. On a Linux host, expand the SCSI Drives tree and click the name of the drive you want to migrate. Click **Choose...** to see the location information.

2. Using a Web browser, log in to the ESX Server machine as root and click **Manage Files**. Use the file manager in the VMware Management Interface to perform all the file copy steps described below.
3. In the file manager, navigate to the location of the source disk files. Select the main disk (`.vmdk` or `.disk`) file for the virtual disk you are migrating, then click **Copy**.
4. Navigate to the **vmfs** folder and open the folder for the VMFS partition where you want to store the virtual disk file. Click **Paste**.

A dialog box appears with the message "You are transferring one or more console virtual disks to a VMFS partition. In order for virtual machines to access these disks, they must be converted to the VMFS format. Although you can convert console disks at any time, it is recommended that you do so now."

The file you are pasting is selected. Click **OK**.

The virtual disk is imported to the VMFS partition.

**Note:** If you do not see the message about transferring disks, there is a problem with the import. Be sure you are pasting to the correct **vmfs** folder.

5. Select the newly imported `.disk` file, then click **Edit Properties**.
6. Change the user and group names in the right-hand column so the file's owner and group match those of the user who will run the virtual machine.

If necessary, change the filename extension to `.disk`.

Click **OK**.

7. Log out, then log back in as the user who will run the new virtual machine.
8. Create a new virtual machine as described in [Creating a New Virtual Machine on page 59](#). When you set the file name for the new virtual machine's disk, be sure to use the virtual disk file you just copied to the VMFS partition.
9. Boot your virtual machine using VMware ESX Server and follow the instructions below for installing VMware Tools and the network driver in the virtual machine.

Some guest operating systems display messages about detecting hardware changes and require you to reboot the virtual machine. This occurs because VMware ESX Server uses an emulation for chipsets and BIOS that is slightly different from those used by other VMware products.



### Installing VMware Tools and the Network Driver in the Guest Operating System

This section describes how to install VMware Tools and the network driver in the guest operating system.

- [Installing VMware Tools and the Network Driver in a Windows 2000 Guest on page 73](#)
- [Installing VMware Tools and the Network Driver in a Windows NT 4.0 Guest on page 74](#)
- [Installing VMware Tools and the Network Driver in a Linux Guest on page 76](#)
- [Installing VMware Tools in a FreeBSD Guest on page 78](#)

Note the following:

- The steps for each guest operating system assume that you are working from a remote console connected to your virtual machine.
- Prepare your virtual machine to install VMware Tools. Choose **Settings > VMware Tools Install**.

This option prepares the CD-ROM drive in the virtual machine to use an ISO image file containing the VMware Tools packages. This image, which appears as a regular CD-ROM disk in the virtual machine, was placed on your server machine when you installed VMware ESX Server.

#### Installing VMware Tools and the Network Driver in a Windows 2000 Guest

1. Choose **Settings > VMware Tools Install**.

This step connects the virtual machine's CD-ROM drive to an ISO image file on the ESX Server machine. If autorun is enabled in your guest operating system (the default setting for Windows operating systems), a dialog box appears after a few seconds. It asks if you want to install VMware Tools. Click **Install** to launch the installation wizard.

If autorun is not enabled, the dialog box does not appear automatically. If it doesn't appear, run `VMwareTools.exe` from the CD-ROM drive (**Start > Run > D: \VMwareTools.exe**, where **D:** is the first CD-ROM drive in your virtual machine) to install VMware Tools.

2. Do one of the following:

- If you configured this virtual machine to use the `v1ance` network driver, go to step 6.

#### Don't Forget VMware Tools

- It is very important that you install VMware Tools in the guest operating system. If you do not install VMware Tools, the graphics environment within the virtual machine is limited to VGA mode graphics (640x480, 16 color).
- With the VMware Tools SVGA driver installed, virtual machines support up to 32-bit displays and high display resolution, with significantly faster overall graphics performance.
- Other tools in the package support time synchronization between server and guest, automatic grab and release of the mouse cursor, copying and pasting between guest and the management workstation, and improved networking performance.

- If you configured this virtual machine to use the `vmxnet` network driver, open the Windows Control Panel (**Start > Settings > Control Panel**) and double-click **Add/Remove Hardware**.
- 3. In the Add/Remove Hardware Wizard, select **Add/Troubleshoot a Device**. Windows searches for Plug and Play devices.
- 4. From the long list of hardware devices, select Ethernet Controller and click **Next**. You should get a message that the drivers for this device are not installed. Click **Finish** to continue.
- 5. Click **Next** on the Upgrade Device Wizard screen. Select **Search for a suitable driver for my hardware device** and instruct Windows to search the CD-ROM drive. Windows should find `D:\vmnet\win2k\oemsetup.inf` (where `D:` is the first CD-ROM drive in your virtual machine). Click **Next** and **Yes** to complete the installation of the VMware network driver.
- 6. When installation is complete, choose **Settings > Cancel Tools Install** to disconnect the ISO image file and return the virtual machine's CD-ROM drive to its original configuration.

### Installing VMware Tools and the Network Driver in a Windows NT 4.0 Guest

1. Choose **Settings > VMware Tools Install**.

This step connects the virtual machine's CD-ROM drive to an ISO image file on the ESX Server machine. If autorun is enabled in your guest operating system (the default setting for Windows operating systems), a dialog box appears after a few seconds. It asks if you want to install VMware Tools. Click **Install** to launch the installation wizard.

If autorun is not enabled, the dialog box does not appear automatically. If it doesn't appear, run `VMwareTools.exe` from the CD-ROM drive (**Start > Run > D:\VMwareTools.exe**, where `D:` is the first CD-ROM drive in your virtual machine) to install VMware Tools.

2. Do one of the following:
  - If you configured this virtual machine to use the `v1ance` network driver, go to step 5.
  - If you configured this virtual machine to use the `vmxnet` network driver, choose **Start > Control Panel > Network > Adapters** and click **Add**.
3. Click **Have Disk** and enter `D:\vmnet\winnt` in the Insert Disk dialog (where `D:` is the first CD-ROM drive in your virtual machine). Click **OK** when VMware

Virtual Ethernet Adapter is displayed in the Select OEM Option dialog. The VMware network driver is installed.

4. Click **Close** in the Adapters dialog box to complete the installation. Windows lets you configure the Internet address for the card.

If you are installing on a virtual machine that was created with VMware Workstation and used networking, you must use an address different from the one the original network configuration used (since that address is still assigned to the now nonexistent virtual AMD card). Or you can change the address assigned to the AMD card at this point.

**Note:** The VMware Virtual Ethernet Adapter driver runs correctly only if you have Service Pack 3 or later installed. If you do not have the proper service pack installed yet, you may get an error message such as: "System Process — Driver Entry Point Not Found; The `\SystemRoot\System32\drivers\vmxnet.sys` device driver could not locate the entry point `NdisGetFirstBufferFromPacket` in driver `NDIS.SYS`." However, even if you get this message, the driver should work if you subsequently install the correct service pack.

5. When installation is complete, and before you reboot, choose **Settings > Cancel Tools Install** to disconnect the ISO image file and return the virtual machine's CD-ROM drive to its original configuration.
6. Reboot the virtual machine.

### Installing VMware Tools and the Network Driver in a Linux Guest

1. Choose **Settings > VMware Tools Install**.

This step connects the virtual machine's CD-ROM drive to an ISO image file on the ESX Server machine.

2. In your Linux guest, become root, mount the VMware Tools virtual CD-ROM, copy the installer file from the virtual CD-ROM to `/tmp`, then unmount the CD-ROM.

```
su
cd /
mount -t iso9660 /dev/cdrom /mnt
cp /mnt/vmware-linux-tools.tar.gz /tmp
umount /dev/cdrom
```

3. Untar the VMware Tools tar file in `/tmp` and install it.

```
cd /tmp
tar xzf vmware-linux-tools.tar.gz
cd vmware-linux-tools
./install.pl
```

**Note:** When installing VMware Tools in some versions of Linux, the installer will need to recompile VMware Tools. For this to work, you will need to have a C compiler installed in the guest. In some cases you may get compiler warning messages during the VMware Tools installation. However, the control panel and drivers will still work correctly.

4. Do one of the following.
  - If you configured this virtual machine to use the `v1ance` network driver, go to step 6.
  - If you configured this virtual machine to use the `vmxnet` network driver, test to be sure that the `vmxnet` driver is installed correctly.

```
insmod vmxnet
```

5. If the driver is installed correctly, you see some informative output but no error messages. In addition, you should now have an entry such as `alias eth0 vmxnet` in the file `/etc/modules.conf` (or `/etc/conf.modules` in Red Hat Linux 6.2).
6. When installation is complete, choose **Settings > Cancel Tools Install** to disconnect the ISO image file and return the virtual machine's CD-ROM drive to its original configuration.

7. If you wish, start X and your graphical environment and launch the VMware Tools background application.

```
vmware-toolbox &
```

**Note:** If you created this virtual machine using only the `vmxnet` driver, you now need to run `netconfig` or another network configuration utility in the virtual machine to set up the virtual network adapter.

### Starting VMware Tools Automatically

You may find it helpful to configure your guest operating system so VMware Tools starts when you start X. The steps for doing so will vary, depending on your Linux distribution and the desktop environment you are running. Check your operating system documentation for the appropriate steps to take.

For example, in a Red Hat Linux 7.1 guest using GNOME, follow these steps.

1. Open the Startup Programs panel in the GNOME Control Center.  
**Main Menu** (the foot in the lower left corner of the screen) > **Programs** > **Settings** > **Session** > **Startup Programs**
2. Click **Add...**
3. In the **Startup Command** field, enter `vmware-toolbox`.
4. Click **OK**, click **OK** again, then close the GNOME Control Center.

The next time you start X, VMware Tools will be started automatically.

### Installing VMware Tools in a FreeBSD Guest

1. Choose **Settings > VMware Tools Install**.

This step connects the virtual machine's CD-ROM drive to an ISO image file on the ESX Server machine.

2. In your Linux guest, become root, mount the VMware Tools floppy, copy the contents of the virtual floppy disk to `/tmp`, then unmount the floppy.

```
su
cd /
mount -t iso9660 /dev/cdrom /mnt
cp /mnt/vmware-freebsd-tools.tar.gz /tmp
umount /dev/fd0
```

3. Untar the VMware Tools tar file in `/tmp` and install it.

```
su
cd /tmp
tar xzf vmware-freebsd-tools.tar.gz
cd vmware-freebsd-tools
./install.pl
```

4. When installation is complete, choose **Settings > Cancel Tools Install** to disconnect the ISO image file and return the virtual machine's CD-ROM drive to its original configuration.
5. Start X and your graphical environment if they are not started yet.
6. In an X terminal, launch the VMware Tools background application.

```
vmware-toolbox &
```

You may run VMware Tools as root or as a normal user.

## Preparing to Use the Remote Management Software

You can manage VMware ESX Server from a remote workstation using the VMware remote console and the VMware Management Interface.

Remote console software is available for Windows and Linux workstations. The remote console lets you attach directly to a virtual machine. You can start and stop programs, change the configuration of the guest operating system and do other tasks as if you were working at a physical computer.

The management interface can be used from any workstation with a compatible browser — Internet Explorer 5.0 or higher or Netscape 4.5 or higher. It gives you a bird's-eye view of all the registered virtual machines on a server and allows you to stop, start, suspend, resume and reset a virtual machine.

**Note:** If you need secure communications between your management workstations and the server, be sure to choose the appropriate security level when you configure ESX Server. For additional details, see the Network Security section in [Authentication and Security Features on page 193](#).

### Registering Your Virtual Machines

If you create your virtual machines using the Virtual Machine Configuration Wizard, they are automatically registered in the file `/etc/vmware/vm-list` on the server's console operating system. The remote management software checks this file for pointers to the virtual machines you want to manage.

If you want to manage virtual machines that you set up in some other way, without using the wizard, you must first register them.

To do so, be sure the virtual machine is powered off. Then, on the overview page of the VMware Management Interface, point to the terminal icon for the virtual machine you want to register and click **Edit Configuration**. Select **Registered** at the top of the Edit Configuration page.

**Note:** Registered virtual machines appear in the list only if their configuration files are stored locally on the ESX Server computer. If the configuration files are stored on an NFS-mounted drive, the virtual machines are not listed.

You can also register the virtual machines from the console operating system. To do so, use this command:

```
vmware-control -s register /<configpath>/<configfile>.cfg
```

To remove a virtual machine from the list, use this command:

```
vmware-control -s unregister \  
/<configpath>/<configfile>.cfg
```

**Note:** Type the whole command on one line. Do not type the backslash.



## Installing the Remote Console Software

Use the package that corresponds to the operating system running on your management workstation and follow the installation steps below.

Installer files are available on the distribution CD-ROM. You may also download the appropriate installer from the Overview page of the VMware Management Interface.

### Windows XP, Windows 2000 or Windows NT 4.0

1. Find the installer file — `VMware-console-1.v.v-xxxx.exe` — on the distribution CD or in the directory where you downloaded it.
2. Double-click `VMware-console-1.v.v-xxxx.exe` to start the installation wizard.
3. Follow the on-screen instructions.

### Linux – RPM Installer

1. Find the installer file — `VMware-console-1.v.v-xxxx.i386.rpm` — on the distribution CD or in the directory where you downloaded it and change to that directory.
2. Become root.  
`su`
3. Run the RPM installer.  
`rpm -Uhv VMware-console-1.v.v-xxxx.i386.rpm`

### Linux – Tar Installer

1. Find the installer file — `VMware-console-1.v.v-xxxx.tar.gz` — on the distribution CD or in the directory where you downloaded it and copy it to the `/tmp` directory or another directory of your choice.
2. Become root.  
`su`
3. Unpack the tar archive.  
`tar xzf VMware-console-1.v.v-xxxx.tar.gz`
4. Change to the directory where the archive was unpacked.  
`cd vmware-console-distrib`
5. Run the installer.  
`./vmware-install.pl`

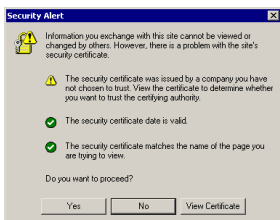
For information on running virtual machines from the remote console, see [Using the Remote Console on page 114](#).

## Accepting the Security Certificate from ESX Server

The first time you use a Web browser to make a secure connection to an ESX Server machine, a dialog box asks whether you want to accept the security certificate presented by the server.

To do so, follow the steps below or take the equivalent steps for your browser version.

### Microsoft Internet Explorer 5.5

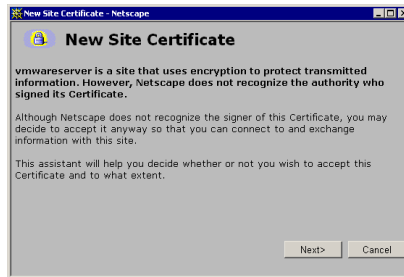


1. A security Alert dialog box appears. To see details of the certificate, click **View Certificate**. To accept the certificate, click **Yes**.

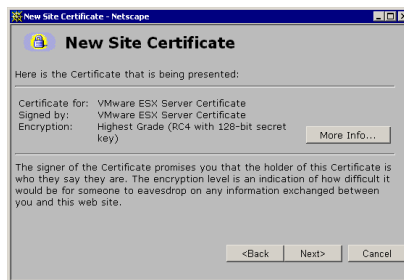


2. Click **Install Certificate...** to launch a wizard that guides you through the process of installing the security certificate.

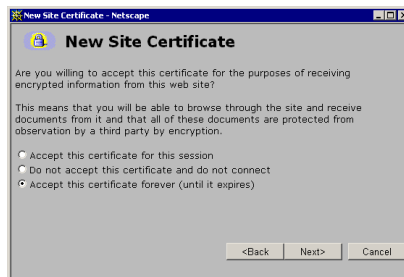
### Netscape Navigator 4.7x on a Windows Management Workstation



1. A New Site Certificate dialog box appears. Click **Next** to begin the process of accepting the certificate.



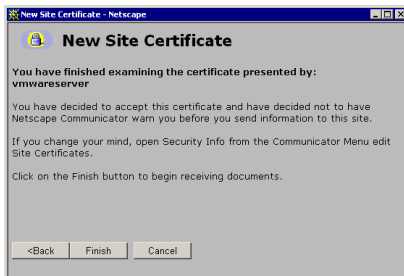
2. View the information about the certificate. Click **Next** to continue.



3. Select **Accept this certificate forever (until it expires)**. Click **Next**.



4. View the fraud warning, then click **Next**.



5. Click **Finish** to complete the process and begin using the security certificate.

# Installing Additional Hardware on the Server

## Installing Hardware for Use by Virtual Machines

After you install the new hardware on your system, use the VMware Management Interface to assign the hardware to the virtual machines.

1. Log in to the management interface as root.
2. Go to the Update Configuration page for the `vmnix` kernel (**Configure System > Allocate Devices > Edit**).
3. Assign the new devices to the virtual machines by selecting the corresponding radio buttons in the Virtual Machines column.
4. Click **Save Configuration**.

## Installing Hardware for Use by the Console Operating System

After you install additional hardware on your system, simply booting or rebooting the machine does not make the console operating system aware of the newly installed hardware.

To make the console operating system aware of newly installed hardware, log in to the console operating system as root, then do one of the following:

- Run the command `kudzu` at a command prompt.
- Manually edit the file `/etc/modules.conf`.

To run `kudzu`:

1. Log in as root on the console operating system.
2. At a command prompt, enter  
`kudzu`
3. The `kudzu` utility detects any new hardware and adds appropriate entries to `/etc/modules.conf`.

If you edit the file `/etc/modules.conf` by hand, add an `alias` line for the new device. For example, if you are adding a new SCSI adapter that uses a driver named `aic7xxx`, add this line:

```
alias scsi_hostadapter aic7xxx
```

# Upgrading from a Previous Version of ESX Server

## Before You Install ESX Server 1.5

There are a few steps you should take before you install ESX Server 1.5 to ensure the best possible upgrade experience.

### Resume and Shut Down Suspended Virtual Machines

If you plan to use virtual machines created under a previous version of ESX Server, be sure they have been shut down completely before you upgrade.

If the virtual machine is suspended, resume it in the earlier release, shut down the guest operating system, then power off the virtual machine.

**Note:** If you attempt to resume a virtual machine that was suspended under a different VMware product or a different version of ESX Server, a message gives you the choice of discarding or keeping the file that stores the suspended state. To recover the suspended state, you must click **Keep**, then resume the virtual machine under the correct VMware product. If you click **Discard**, you can power on normally, but the suspended state is lost.

### Commit or Discard Changes to Undoable Disks

If you plan to use existing virtual machines that have undoable disks, commit or discard any changes to the virtual disks before you remove the release you used to create them.

Resume or power on the virtual machine in the earlier release, shut down the guest operating system, power off the virtual machine and either commit or discard changes to the undoable disk when prompted.

### Back Up Virtual Machines

As a precaution, back up the virtual machine files — including the `.disk` and `.cfg` files — for any existing virtual machines you plan to migrate to ESX Server 1.5.

**Caution:** The upgrade script used to upgrade from ESX Server 1.0 and ESX Server 1.1 to ESX Server 1.5 overwrites information related to sharing an Ethernet adapter between virtual machines and the console operating system. If you are using this functionality, you must set it up again after you upgrade. For details, see [Sharing the Console Operating System's Network Adapter with Virtual Machines on page 226](#).

### Upgrading from ESX Server 1.1 to ESX Server 1.5

To upgrade from ESX Server 1.1 to ESX Server 1.5, use the installation CD-ROM.

1. Insert the installation CD into the server's CD-ROM drive.
2. Reboot the computer and log in as root.
3. At the first installer screen, choose **Upgrade from ESX Server 1.0/1.1**.
4. You are asked if you have a driver disk provided by VMware for a device that is not handled by drivers in this release of ESX Server.  
  
If you do not have a driver disk, choose No and continue with the installation.  
  
If you have a driver disk from VMware, put the driver disk into the floppy drive and choose Yes.
5. If you do not have enough swap space for the new console operating system, the installer asks you where to place a new swap file. Accept the default location unless you have a specific reason for using a different one.
6. The installer upgrades your ESX Server installation.
7. When the upgrade completes and displays the final screen, reboot. The machine keeps the device allocations that you previously set up.
8. After the server reboots, from your management workstation use a supported Web browser and go to:

`http://<hostname>/vmware/config`

9. Log in as root, then go to the Network Configuration (**Configure System > Network Configuration**) and Security Settings (**Configure System > Security Settings**) pages to ensure that the current settings are appropriate. The Network Configuration page is new in ESX Server 1.5.

Go to the Boot Configuration page (**Configure System > Update Boot Configuration > Edit**) and adjust the amount of memory allocated to the console operating system. Change the number to 128MB for managing up to three or four virtual machines. Increase this to 192MB for eight virtual machines, 272MB for 16 virtual machines, 384MB for 32 virtual machines or 512MB for more than 32 virtual machines. For background, see [Sizing Memory on the Server on page 249](#).

### Upgrading from ESX Server 1.0 to ESX Server 1.5

To upgrade from ESX Server 1.0 to ESX Server 1.5, use the installation CD-ROM.

1. Insert the installation CD into the server's CD-ROM drive.



2. Reboot the computer and log in as root.
3. At the first installer screen, choose Upgrade from ESX Server 1.0/1.1.
4. You are asked if you have a driver disk provided by VMware for a device that is not handled by drivers in this release of ESX Server.  
  
If you do not have a driver disk, choose No and continue with the installation.  
  
If you have a driver disk from VMware, put the driver disk into the floppy drive and choose Yes.
5. If you do not have enough swap space for the new console operating system, the installer asks you where to place a new swap file. Accept the default location unless you have a specific reason for using a different one.
6. The installer upgrades your ESX Server installation.
7. When the upgrade completes and displays the final screen, reboot.
8. After the server reboots, from your management workstation use a supported Web browser and go to:

`http://<hostname>/`

9. Log in as root, then start the ESX Server Setup Wizard by clicking the Setup Wizard link at the top of the page. Each page of the wizard includes instructions for the actions you need to take there.

On the Boot Configuration page, adjust the amount of memory allocated to the console operating system. Change the number to 128MB for managing up to three or four virtual machines. Increase this to 192MB for eight virtual machines, 272MB for 16 virtual machines, 384MB for 32 virtual machines or 512MB for more than 32 virtual machines. For background, see [Sizing Memory on the Server on page 249](#).

Be sure to enter your new serial number at the appropriate page.

### Setting File Permissions on Existing Virtual Disk Files

If you are upgrading to ESX Server 1.5 on a computer that has virtual machines created under ESX Server 1.0 or 1.1, be sure to set permissions appropriately on all virtual disk files stored on a VMFS partition. Support for permissions on VMFS files is a new feature in version 1.5.

All your VMFS files will initially be owned by root and have permissions of 000. You must at least change the permissions of the files so they are readable and writable by root. You may wish to change the owner as well. You can use the file manager of the management interface to change the owner and permissions.

Alternatively, on the console operating system, you can use the `vmkfstools` command, or you can change the permissions and owner directly on the files in `/vmfs` using the Linux `chmod` and `chown` commands.

### Updating Virtual Machine Configurations

After you upgrade from ESX Server 1.0 or ESX Server 1.1 to ESX Server 1.5, you may want to update one setting in each virtual machine's configuration file to take advantage of new virtual hardware features supported by ESX Server 1.5. The key new feature is support for up to 3.6GB of memory inside the virtual machine.

**Note:** If you are using virtual disks in nonpersistent mode, you must temporarily switch to persistent mode to make these changes. If you are using repeatable resume, you must then recreate your resume point as described in [Enabling Repeatable Resumes on page 191](#).

To take advantage of the new virtual hardware features, follow these steps:

1. Log in to the VMware Management Interface as a user with proper permissions to manage the virtual machines.
2. On the overview page, point to the terminal icon for each virtual machine in turn and choose **Edit Configuration**. On the Configure VM page, click **Use Text Editor**.
3. Find the line that begins with `config.version`. Change it to  
`config.version = 6`
4. Click **Save Changes**.
5. Click **VMs on <hostname>** to return to the Overview page.
6. Repeat the process for each virtual machine.
7. Launch the remote console and power on each virtual machine in turn.
8. As the virtual machine starts, you see a dialog box with the message "The CMOS of this virtual machine is incompatible with the current version of VMware ESX Server. A new CMOS with default values will be used instead."  
Click **OK**.
9. The guest operating system may detect new virtual hardware and install drivers for it. Respond to any messages as you would if upgrading the hardware on a physical computer.
10. When the guest operating system is running, install the new version of VMware Tools, following the instructions in [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

# 3

## **Running VMware ESX Server**

## Running VMware ESX Server

The following sections describe various aspects of running ESX Server:

- [Using the VMware Management Interface on page 94](#)
  - [Editing a Virtual Machine's Configuration Remotely on page 99](#)
  - [Managing the VMware ESX Server File System from the Management Interface on page 99](#)
  - [Viewing and Changing VMkernel Settings on page 104](#)
  - [Deleting a Virtual Machine from the Management Interface on page 106](#)
  - [Using Disk Modes on page 108](#)
  - [Monitoring System Status on page 109](#)
  - [Setting the MIME Type in Netscape Navigator 4.x on page 111](#)
  - [See Setting the MIME Type in Netscape 6 and Mozilla on page 112.](#)
- [Using the Remote Console on page 114](#)
  - [Starting the Remote Console on Windows on page 114](#)
  - [Starting the Remote Console on Linux on page 114](#)
  - [Running a Virtual Machine Using the Remote Console on page 115](#)
  - [VMware Tools Settings on page 117](#)
  - [Installing New Software Inside the Virtual Machine on page 119](#)
  - [Cutting, Copying and Pasting on page 119](#)
  - [Suspending and Resuming Virtual Machines on page 120](#)
  - [Shutting Down a Virtual Machine on page 121](#)
- [Rebooting or Shutting Down the Server on page 122](#)
- [Using SNMP with ESX Server on page 125](#)
  - [Configuring the ESX Server SNMP Agent on page 129](#)
  - [Configuring SNMP Management Software on page 131](#)
  - [Configuring SNMP Security on page 132](#)
  - [Using SNMP with Guest Operating Systems on page 132](#)
  - [VMware ESX Server SNMP Variables on page 132](#)
- [Backing Up Virtual Machines on page 140](#)
- [The VMware Guest Operating System Service on page 144](#)

- [Synchronizing the Time Between the Guest and Console Operating Systems on page 144](#)
- [Shutting Down and Restarting a Virtual Machine on page 145](#)
- [Executing Commands When ESX Server Requests the Guest Service to Halt or Reboot a Virtual Machine on page 146](#)
- [Passing a String from the Console Operating System to the Guest Operating System on page 147](#)

## Using the VMware Management Interface

The following sections describe how to use the management interface:

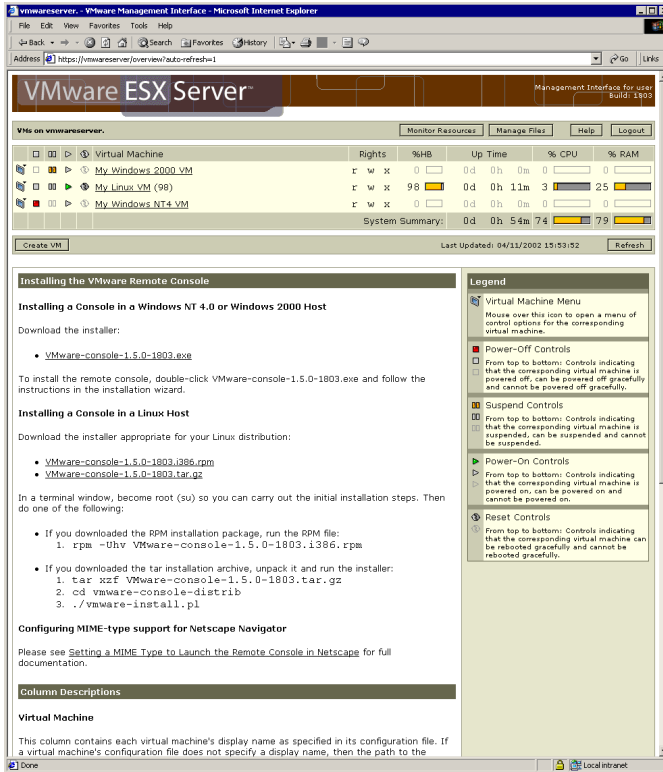
To use the VMware Management Interface, you must run Internet Explorer 4.0 or higher, Netscape Navigator 4.5 or higher, Netscape 6, or Mozilla 0.9.4 or higher. If you are using Netscape Navigator, Netscape or Mozilla, check the advanced preferences (**Edit > Preferences > Advanced**) to be sure JavaScript and style sheets are both enabled. You need to know the host name or IP address of the server you want to monitor.

You should use the VMware Management Interface from a management workstation, not from the server machine where ESX Server is installed. Running X on your server's console operating system is not recommended.











**Note:** The file system browser feature of the management interface must be used in Microsoft Internet Explorer 5.0 or higher, Netscape 6, or Mozilla 0.9.4 or higher. It does not function correctly in Netscape Navigator 4.x.

The URL to connect to the server is `http://<hostname>/overview/`.

## Running VMware ESX Server



The information and controls in the VMware Management Interface are arranged in columns containing symbols, some of which are similar to those on a CD player, and text. These symbols and icons appear on the Overview, Details and Event Log pages.

Item	Description
	<p>Hold the mouse over the icon to display a menu of options for the virtual machine, or click to launch a remote console. Netscape users must define a MIME type for the console first; Internet Explorer is automatically configured when the remote console is installed.</p> <p>The menu includes the following commands. Depending on your permissions and the state of the virtual machine, some options may not be available.</p> <p><b>Launch Remote Console</b> – launches the remote console. This is the same as clicking .</p> <p><b>View Details</b> – opens the Details page for this virtual machine. This is the same as clicking the display name link in the Virtual Machine column.</p> <p><b>View Event Log</b> – opens the Event Log page for this virtual machine. This is the same as clicking the Event Log link on the Overview page.</p> <p><b>Power-Off</b> – gracefully powers off the guest operating system and the virtual machine. This is the same as clicking .</p> <p><b>Suspend</b> – suspends a running virtual machine or resumes a suspended virtual machine. This is the same as clicking .</p> <p><b>Power-On</b> – powers on a stopped virtual machine or resumes a suspended virtual machine. This is the same as clicking .</p> <p><b>Reset</b> – gracefully resets the guest operating system and the virtual machine. This is the same as clicking .</p> <p><b>Force Power-Off</b> – shuts down the virtual machine immediately. This is the same as turning off the power to a physical computer.</p> <p><b>Force Reset</b> – resets the virtual machine immediately. This is the same as pressing the reset button on a physical computer.</p>
	<p>Click to gracefully power off the virtual machine. ESX Server closes any open applications and shuts down the guest operating system before powering off the virtual machine. When this icon is red, the virtual machine has been powered off.</p>
	<p>Click to suspend a running virtual machine or resume a suspended virtual machine. When this icon is orange, the virtual machine has been suspended.</p>
	<p>Click to power on a stopped virtual machine or to resume a suspended virtual machine. When this icon is green, the virtual machine is running.</p>
	<p>Click to gracefully reset a running virtual machine. ESX Server closes any open applications and shuts down the guest operating system before resetting the virtual machine.</p>



Item	Description
Virtual Machine	The path to the configuration file for the virtual machine; if a display name for the virtual machine is specified in the configuration file, then that name appears here instead. Click the link for more details about the virtual machine.
Rights	Rights represent the permissions you have for each configuration file on the physical machine. The available permissions are <b>read</b> , <b>write</b> and <b>execute</b> .
% HB	% HB is the average percentage of heartbeats received by a virtual machine during the minute prior to the last page update. Heavily loaded guest operating systems may not send 100% of the expected heartbeats, even though the system is otherwise operating normally; in general, only when the heartbeat percentage drops to zero should the virtual machine or guest operating system be considered unhealthy. Note that if VMware Tools is not installed or is not running, the guest operating system does not send any heartbeats to its virtual machine and this meter is disabled.
Up Time	The length of time the virtual machine has been running in days, hours, minutes and seconds.
% CPU	The average percentage of the physical computer's processor capacity the virtual machine used during the final minute before the page was last updated. <b>Note:</b> This column appears on the Overview page only.
% RAM	The average percentage of the physical computer's memory the virtual machine used during the final minute before the page was last updated. <b>Note:</b> This column appears on the Overview page only.
System Summary	The total up time for the system, as well as processor consumption and memory usage for <b>all</b> processes running on the system.
Event Log	Opens the Event Log page, showing more entries from the virtual machine's log file. This link is available only on the Details page for a virtual machine.

In addition, the following buttons appear on most or all of the pages in the management interface.

**Update** – This button refreshes or reloads the current page. To avoid conflicts with other users, click this button before you perform an operation like shutting down, suspending, resuming or starting a virtual machine. The Update button does not appear on the New VM page.

**Logout** – This button logs you out of the management interface. Click Logout to return to the Login page.

**Help** – This button connects you to the main page for ESX Server online documentation.

**Create VM** – This button appears on the Overview page. It opens the New VM page, where you create new virtual machines. [See Creating a New Virtual Machine on page 59.](#)

**Configure System** – This button appears on the Overview page. It opens the VMware ESX Server Configuration page, where you can change the settings for your VMware ESX Server computer. [See Using the Setup Wizard to Configure Your Server on page 33.](#)

**Manage/Monitor Resources** – This button appears on the Overview page. It opens the Resource Monitor page, which contains an overview of how the physical machine's processors, memory and network bandwidth are being utilized by the virtual machines.

If you are logged in as the root user, this button is labeled Manage Resources, and it allows you to tailor the resources for each virtual machine, increasing or decreasing the virtual machine's share of processor, memory and network resources.

For more information, see [Resource Management on page 231.](#)

**Edit VM Configuration** – This button appears on a virtual machine's Details page. It takes you to the Configure VM page, where you can change many of a virtual machine's configuration settings. This button is active only when the virtual machine is powered off.

**Delete VM Configuration** – This button lets you delete a virtual machine or just its configuration, provided the virtual machine is powered off. When you click Delete VM Configuration, the Delete VM page appears.

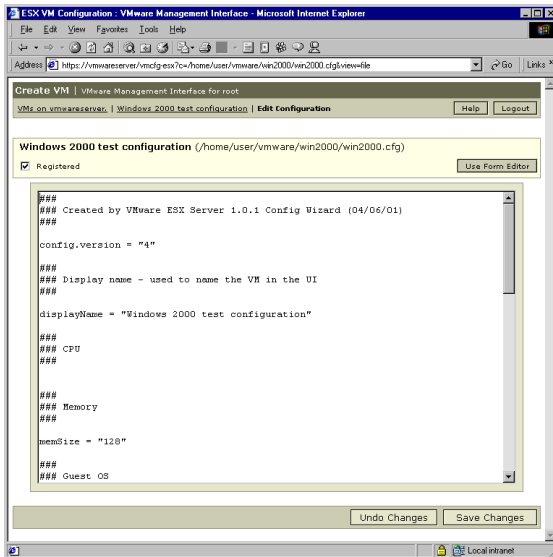
When a virtual machine is running, the Overview page displays its ID number in parentheses after the machine's name.

### Editing a Virtual Machine's Configuration Remotely

You can edit a virtual machine's configuration file remotely from the VMware Management Interface. This lets you change more elements of a virtual machine's configuration than you could on the Configure VM page and it saves you from having to use a text editor.

Modifying a configuration file this way is recommended for advanced users only. The virtual machine must be powered off. You should back up your virtual machine's configuration file before modifying it this way.

In the VMware Management Interface, on the Details page for the virtual machine, click Edit VM Configuration. The Configure VM page appears. Click the Use Text Editor link. The Edit Configuration page appears, displaying the contents of the virtual machine's configuration file.



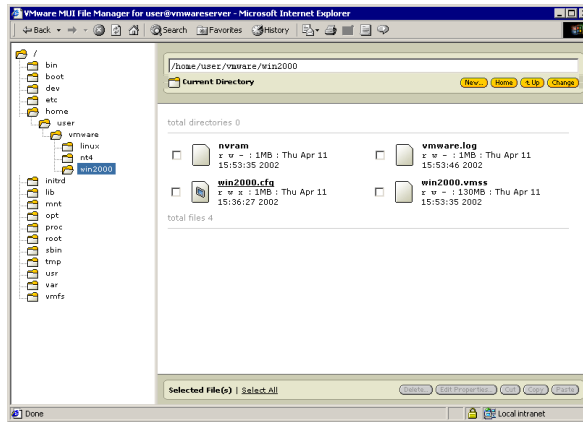
After you make your changes, click Save Changes.

### Managing the VMware ESX Server File System from the Management Interface

Using the VMware Management Interface, you can manage the file system of your VMware ESX Server machine remotely. Use the file manager to change the permissions of any file on the physical machine, create new directories on the physical

machine or cut, copy, paste and delete files as you would if you were working directly on the file system itself. To use the file manager, click Manage Files on the overview page of the management interface. To go directly to the file system browser, point your Web browser to `http://<hostname>/showdir`.

**Note:** For best results, open the file manager in Microsoft Internet Explorer 5.0 or higher, Netscape 6, or Mozilla 0.9.4 or higher. The file manager does not function correctly in Netscape Navigator 4.x. (The version of Netscape Navigator that ships with the console operating system does not work correctly with the file manager.)







In the left pane of the file manager, click a folder to display its contents.

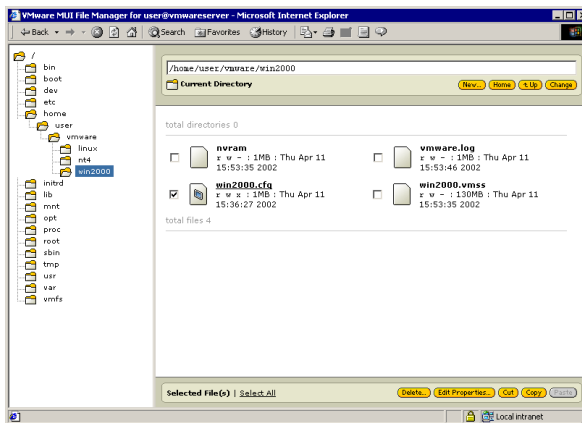
**Note:** The tree view may fail to load or may only partially load when viewed with Netscape Navigator 6 or Mozilla. To restore the proper view, right-click in the left pane, then choose **Reload Frame** from the context menu.

**Note:** The overview page may appear in place of the tree view or the main directory view when viewed with Netscape Navigator 6. To restore the proper view, clear the browser's disk and memory cache, then reload the file manager.

File and folder icons change color to indicate their state when you select them and perform certain actions, such as copy and paste.

Some file and folder icons have special meanings.

Item	Description
	This icon identifies a virtual machine configuration file. If you click the filename or icon for a configuration file, the Edit Configuration page for the corresponding virtual machine opens in a browser window.
	This icon identifies a virtual disk file on a VMFS file system.
	This icon identifies a set of files on the console operating system that hold a virtual disk in the format used by VMware Workstation and VMware GSX Server.
	This icon identifies a VMFS file system.



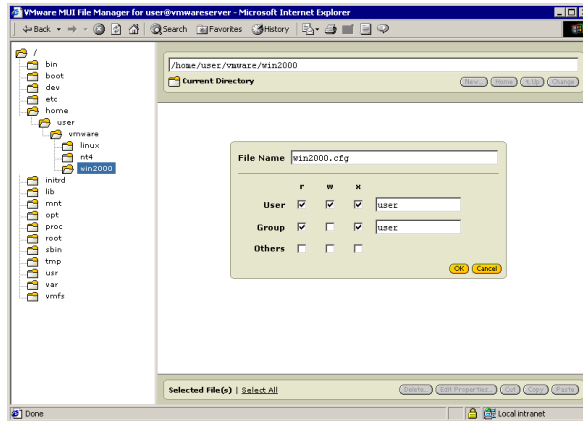
To perform an action on a file or folder (directory), click the check box beside its listing, then click the appropriate yellow button at the bottom of the screen to delete, edit properties, cut or copy.

After you have cut or copied a file or folder, you may then paste it into the same or a different folder. If you copy a file or folder, then paste it into the same folder, the new file or folder is renamed, with `copy_0£_` before the original name. You may then select it and use **Edit Properties** to give it a name of your choice.

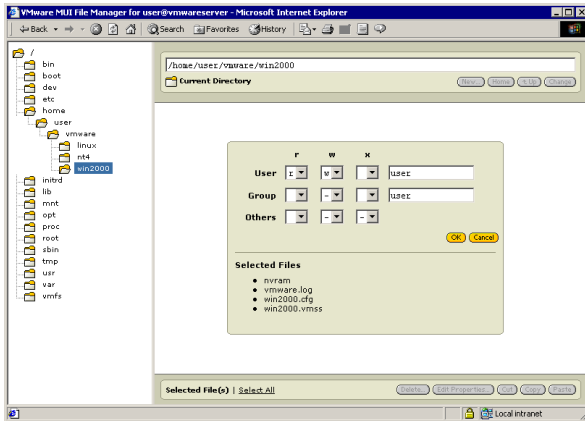
When you start a long-running operation — for example, pasting a file larger than 10MB after a copy or moving it between logical file systems — a progress bar appears so you can track the progress of the operation.

## Running VMware ESX Server

When you copy and paste or cut and paste a virtual disk file from the VMFS file system to the console operating system's file system, or vice versa, the file manager uses `vmkfstools` to import or export the file, translating the format appropriately. Among other things, this means a virtual disk larger than 2GB will be split into multiple files when it is moved from a VMFS disk or array to the console operating system's file system. For background on `vmkfstools`, see [Using vmkfstools on page 199](#).

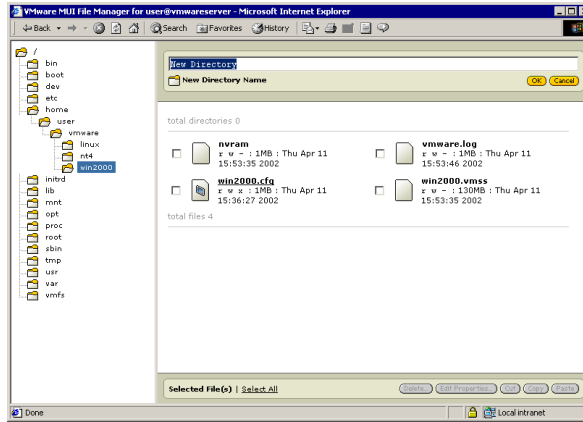


After selecting a file or folder and clicking **Edit Properties**, you can change its name and permissions. When you are finished, click **OK** to apply the changes.



If you select more than one file or folder, you can change permissions for all the files at once. Any changes you make, using the drop-down lists in the file manager, apply to all the files you have selected.

- A letter, corresponding to the letter at the top of the column (read, write or execute), indicates that the setting is the same for all files and it does grant the permission indicated by the letter.
- A hyphen (–) indicates that the setting is the same for all files and it does not grant permission.
- A blank space indicates that the setting is not the same for all files.



Use the top pane of the file manager to navigate the directory structure and create new directories.

To create a new directory, click **New...**, enter the name for the new directory, then click **OK**.

### Viewing and Changing VMkernel Settings

When you configure the VMware ESX Server computer (see [page 33](#)), various system parameters are assigned predetermined values. These parameters control settings for memory, the processor and networking, for example, and affect the running of virtual machines. You can view these settings from the management interface.

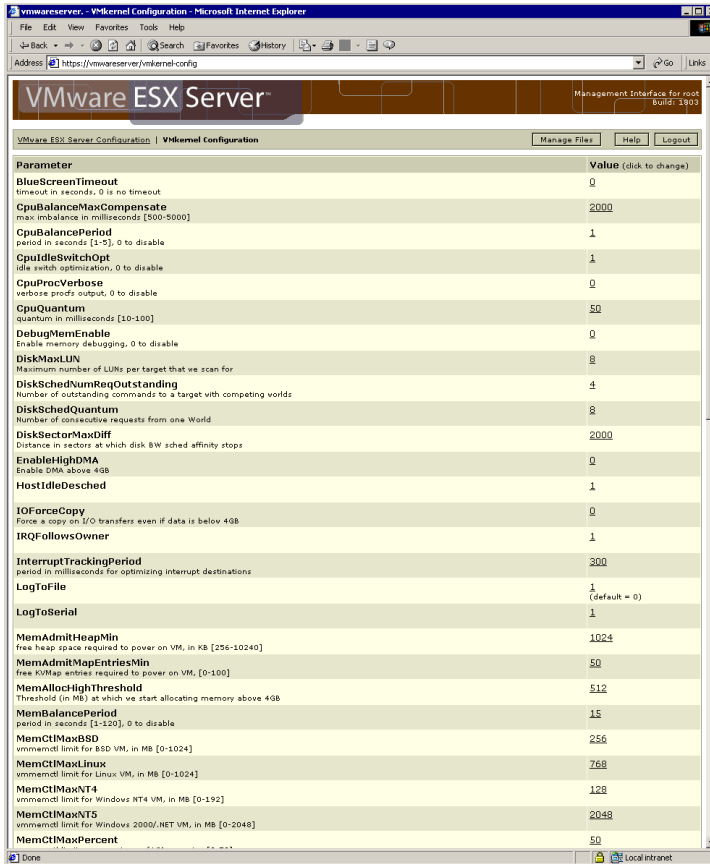
If you are logged in as the root user, you can change the values for these parameters. Changing these values can help fine tune the running of virtual machines.

**Note:** Some configuration settings shown on this page are described in the ESX Server manual and may be changed as described in the manual. In most cases, however, you should not modify these settings unless a VMware technical support engineer suggests that you do so.

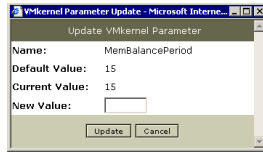
To view and change VMkernel configuration settings, on the VMware ESX Server Configuration page (<http://<hostname>/vmware/config/>), click **VMkernel Configuration**. Or point your browser to <http://<hostname>/vmkernel-config>.



## Running VMware ESX Server



To change the setting for a VMkernel configuration parameter, click the link for the value. The Update VMkernel Parameter window opens on top of the VMware Management Interface window.



In the **New Value** entry field, type the value for the parameter and click **Update**. The window closes and the updated parameter appears on the VMkernel Configuration page.

### Deleting a Virtual Machine from the Management Interface

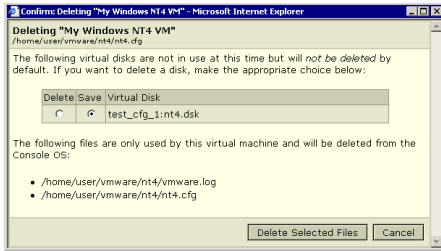
You can delete a virtual machine only if you are an administrator, if you are the owner of the configuration file or if you have permissions that allow you to modify or change the configuration file or the directory where the configuration file is located.

When you delete a virtual machine, the files associated with it — that is, the files located in the same directory — are deleted. These files include the virtual machine's configuration file (the `.vmx` file), its log file and its `nvr.am` file. The redo log and any lock files are not deleted.

Any virtual disks that are not associated with another registered virtual machine on the computer can be deleted as well, or you can save any or all of them for future use. The directory containing these files is also deleted if it is empty. If any disk files or other files are not deleted, the directory is not deleted.

To delete a virtual machine, complete the following steps.

1. In the VMware Management Interface, find the virtual machine you want to delete and follow the link to its Details page.
2. If the virtual machine is powered on or suspended, power it off.
3. Click **Delete VM Configuration**. The Delete VM Confirmation window opens.



4. You see a list of all the files that are to be deleted. For each disk file not associated with another registered virtual machine on this computer, choose one of the following:

- To save a virtual disk file, select **Save**.
- To delete a virtual disk file, select **Delete**.

**Note:** Virtual disk files associated with another registered virtual machine do not appear in this window.

5. When you are ready to delete the virtual machine, click **Delete Selected Files**. You return to the Overview page.

## Using Disk Modes

You can use the Configure VM page of the VMware Management Interface to change the disk mode for the disks used by your virtual machine.

1. Connect to the server that hosts the virtual machine as a user who has rights to administer the virtual machine. The virtual machine should be powered off.
2. Move your mouse pointer over the terminal icon beside the name of the virtual machine you want to modify.
3. Choose **Edit VM Configuration**.
4. Find the listing for the drive you want to change.
5. Choose the appropriate option for persistent, nonpersistent, undoable or append disk mode from the drop-down list, then click **Save Changes**.

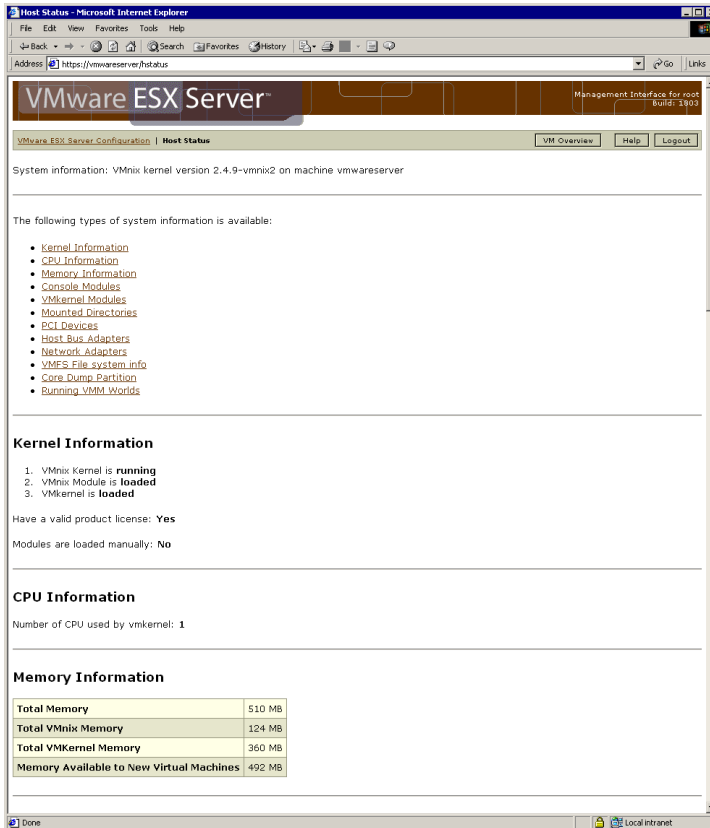
ESX Server can use disks in four different modes: persistent, nonpersistent, undoable and append.

- **Persistent:** Persistent disks behave exactly like conventional disk drives on a computer. All writes to a persistent disk are written out permanently to the disk as soon as the guest operating system writes the data.
- **Nonpersistent:** All changes to a nonpersistent mode disk are discarded after that ESX Server session is powered down.
- **Undoable:** When you use undoable mode, you have the option later of keeping or discarding changes you have made during a working session. Until you decide, the changes are saved in a redo-log file.
- **Append:** VMware ESX Server supports an additional append mode for virtual disks stored as VMFS files. Like undoable mode, append mode maintains a redo log. However, in this mode, no dialog appears when the virtual machine is powered off to ask whether you want to commit changes. All changes are continually appended to the redo log. At any point, the changes can be undone by removing the redo log. You should shut down the guest operating system and power off the virtual machine before deleting that virtual machine's redo log. You can also commit the changes to the main virtual disk file using the `commit` option in `vmkfstools`. See [Using vmkfstools on page 199](#) for details.

## Monitoring System Status

All users can get an overview of system status on the overview page of the management interface. The root user can monitor system status in more detail.

The Host Status page provides summary information on multiple topics. To view this information, from the overview page click **Configure System** then click **Machine Status**.

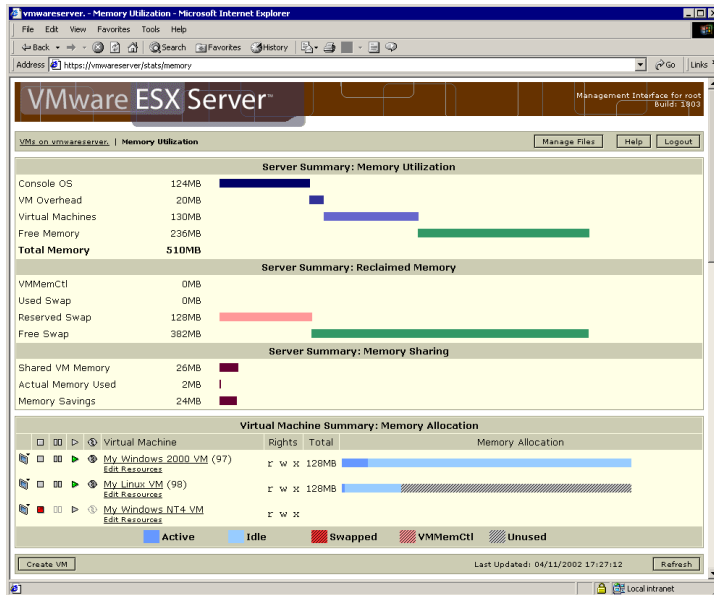


Click a link at the top of the page to go directly to a specific section.

The Memory Utilization page provides information on the current use of RAM by the physical computer and the virtual machines running on it — in graphical and

## Running VMware ESX Server

numerical form. To view this information, from the overview page click **Configure System**, then click **Memory Utilization**.



The Server Summary section at the top shows systemwide information. The Virtual Machine Summary section below it shows information for particular virtual machines. A detailed explanation of the information is at the bottom of the page.

To update the display, click **Refresh**.

### Setting the MIME Type in Netscape Navigator 4.x

If you are using Netscape Navigator 4.x and want to launch a remote console from the VMware Management Interface, as described above, you must first set a MIME type for the remote console program.

#### Windows

In Netscape Navigator on Windows, follow these steps to set the MIME type.

1. Use the browser to connect to the server you want to manage.
2. Click the terminal icon for the virtual machine you want to view in a remote console.
3. A dialog asks what you want to do with the file. Click **Pick App**.
4. Another dialog lets you enter the path to the application or browse to it.  
Fill in the path or browse to the remote console program.

The default path is

```
C:\Program Files\VMware\Programs\Console\RemoteConsole.exe" -o "%1
```

5. Your browser is now set to launch the remote console when you click the terminal icon in the future.

#### Linux

In Netscape Navigator on Linux, follow these steps to set the MIME type.

1. Select **Edit > Preferences....**
2. Expand **Navigator**.
3. Highlight **Applications**.
4. Click **New**.  
An input dialog is displayed.
5. Fill in the **Description** field with `VMware remote console`.
6. Fill in **MIME Type** with `application/x-vmware-console`.
7. Leave **Suffixes** blank.
8. Select **Application**.
9. Fill in **Application** with the path to the remote console program or click **Choose** to navigate to the program on your computer. The default path is  
`/usr/bin/vmware-console -o %s > /dev/null 2>&1;`
10. Click **OK** to close the input dialog.
11. Click **OK** to close the preferences dialog.

### Setting the MIME Type in Netscape 6 and Mozilla

If you are using Netscape 6 or Mozilla and want to launch a remote console from the VMware Management Interface, as described above, you must first set a MIME type for the remote console program.

#### Windows

In Netscape or Mozilla on Windows, follow these steps to set the MIME type.

1. Write a short batch file that contains the following line:

```
"<path_to_vmwareConsole>" -o %1
```

The default path is

```
C:\Program Files\VMware\Programs\Console\vmwareConsole.exe.
```

Save the file in a location of your choice as

```
vmwareConsole-helper.bat.
```

2. Use the browser to connect to the server you want to manage.
3. Click the terminal icon for the virtual machine you want to view in a remote console.
4. A dialog asks what you want to do with the file. Click **Pick App**.
5. Another dialog lets you enter the path to the application or browse to it.  
Fill in the path or browse to `vmwareConsole-helper.bat`.
6. Your browser is now set to launch the remote console when you click the terminal icon in the future.

#### Linux

In Netscape or Mozilla on Linux, follow these steps to set the MIME type.

1. Write a short shell script that contains the following two lines:

```
#!/bin/sh
```

```
"<path_to_vmware-console>" -o $1 > /dev/null 2>&1;
```

The default path is `/usr/bin/vmware-console`.

Save it in a location of your choice as `vmware-console-helper.sh`.

2. Change to the directory where you saved the file and use `chmod` to give yourself permission to execute the file.  

```
chmod +x vmware-console-helper.sh
```
3. Select **Edit > Preferences...**
4. Expand **Navigator**.



5. Highlight **Helper Applications**.
6. Click **New Type...**  
An input dialog is displayed.
7. Fill in the **Description of type** field with `VMware remote console`.
8. Fill in **MIME Type** with `application/x-vmware-console`.
9. Leave **File extension** blank.
10. Select **Application**.
11. Fill in **Application** with the path to `vmware-console-helper.sh` or click **Choose** to navigate to the shell script on your computer.
12. Click **OK** to close the input dialog.
13. Click **OK** to close the preferences dialog.

## Using the Remote Console

The remote console gives you a direct window into an individual virtual machine running under VMware ESX Server. Remote console software is available for Windows XP, Windows 2000, Windows NT and Linux management workstations. For instructions on installing the software, see [Installing the Remote Console Software on page 81](#).

### Starting the Remote Console on Windows

1. Start the remote console program.

**Start > Programs > VMware > VMware Remote Console**

2. A dialog box asks for the information needed to connect you to the virtual machine. Fill in the blanks with

- The host name (or IP address)
- Your user name
- Your password

Click **Connect**.

3. When the connection is made, a dialog box displays the paths to the configuration files of virtual machines registered on the server. Select the virtual machine you want to connect to, then click **OK**.

### Starting the Remote Console on Linux

1. Start the remote console program.

`vmware-console`

2. A dialog box asks for the information needed to connect you to the virtual machine. Fill in the blanks with

- The host name (or IP address)
- Your user name
- Your password

Click **Connect**.

3. When the connection is made, a dialog box displays the paths to the configuration files of virtual machines registered on the server. Select the virtual machine you want to connect to, then click **OK**.

### Running a Virtual Machine Using the Remote Console

When you view your virtual machine through a remote console, it behaves much like a separate computer that runs in a window on your computer's desktop.

Instead of using physical buttons to turn this computer on and off, you use buttons at the top of the VMware console window. You can also reset the virtual machine, suspend a virtual machine and resume a suspended virtual machine.



*This virtual machine is powered off*



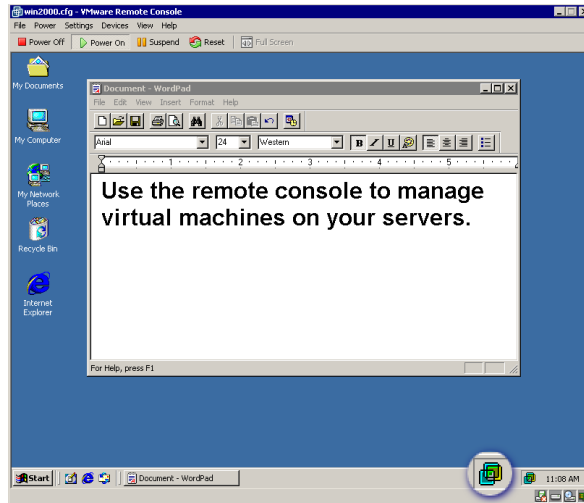
*This virtual machine is powered on*



*This virtual machine is suspended*

**Note:** The illustrations above show the toolbar from a remote console running on a Windows management workstation. If you are running the remote console on a Linux management workstation, the appearance of the toolbar is somewhat different, but the same functions are available.

## Running VMware ESX Server

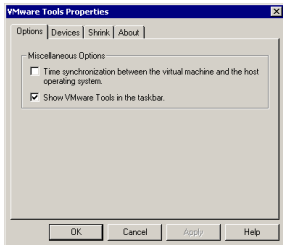


*When VMware Tools for Windows is running, the VMware Tools icon appears in the system tray*

## VMware Tools Settings

The following description of the settings for VMware Tools is based on a Windows 2000 guest operating system. Similar configuration options are available in VMware Tools for other guest operating systems.

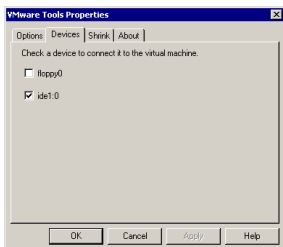
1. To open the VMware Tools control panel, double-click the VMware Tools icon in the virtual machine's system tray. The VMware Tools Properties dialog appears.



2. On the Options tab, you can specify whether you want to synchronize the time between the virtual machine and the console operating system. You can also specify whether you want to display the VMware Tools icon in the system tray.

If you choose not to display the VMware Tools icon in the system tray, you can launch the control panel from the Start menu (**Start > Settings > Control Panel > VMware Tools**).

3. To enable or disable removable devices, click the Devices tab.

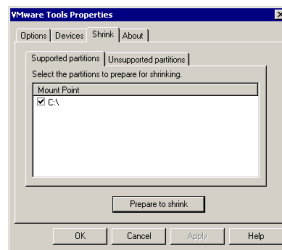


The devices you can enable or disable include the server machine's floppy disk drive and the CD-ROM drive. You can also set these options from the Devices menu of the ESX Server remote console window.

4. The Shrink tab lets you prepare to export a virtual disk to VMware GSX Server using the smallest possible disk files. This step is an optional part of the export process.

Virtual disks on ESX Server take up the full amount of disk space indicated by the virtual disk's size. In other words, the `.disk` file for a 4GB virtual disk occupies 4GB of disk space.

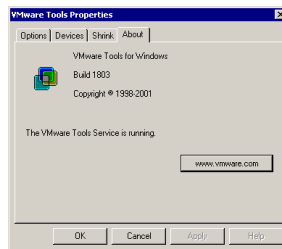
GSX Server works differently. Under GSX Server, virtual disk files start small — only as big as needed to hold the data stored on the virtual disk — and grow as needed up to the designated maximum size.



If you plan to export a virtual disk for use under GSX Server, click the Shrink tab, be sure there is a check beside the name of the disk you plan to export, then click **Prepare to shrink**.

**Note:** When you export the virtual disk (using the file browser in the management interface or the `vmkfstools` program), a single virtual disk may be exported to multiple `.disk` files.

5. On the About tab, you see information about the version of VMware Tools installed in the virtual machine. Click the [www.vmware.com](http://www.vmware.com) button to go to the VMware home page on the Web.



### Installing New Software Inside the Virtual Machine

Installing new software in an ESX Server virtual machine is just like installing it on a regular computer.

If you are using physical media, you need to have access to the ESX Server computer to insert installation CD-ROM discs or floppy disks into the server's drives.

You may use image files in place of physical floppy disks and CD-ROM discs. To connect the virtual drive to a floppy or ISO image, use the Devices menu and edit the settings for the drive you want to change.

The following steps are based on using a Windows guest operating system and physical media. If you are using a Linux guest operating system — or if you are using ISO or floppy image files — some details are different.

1. Be sure you have started the virtual machine and, if necessary, logged on. Check the Devices menu to be sure the virtual machine has access to the CD-ROM and floppy drives.
2. Insert the installation CD-ROM or floppy disk into the proper drive. If you are installing from a CD-ROM, the installation program may start automatically.
3. If the installation program does not start automatically, click the Windows **Start** button, go to **Settings > Control Panel**, then double-click **Add/Remove Programs** and click **Add New Programs**. Follow the instructions on screen and in the user manual for your new software.

### Cutting, Copying and Pasting

Be sure you have installed and started VMware Tools in your virtual machine.

In a Windows guest operating system, you see a VMware Tools icon in the system tray when VMware Tools is running.

When VMware Tools is running, you can copy and paste text between applications in the virtual machine and on your management workstation or between two virtual machines. Use the normal hot keys or menu choices to cut, copy and paste.

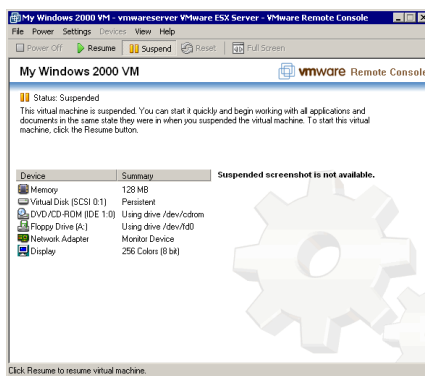
## Suspending and Resuming Virtual Machines

You can save the current state of your virtual machine. Then the resume feature lets you quickly pick up work right where you stopped — with all running applications in the same state they were at the time you suspended the virtual machine.

**Note:** You cannot suspend a virtual machine configured to use more than 2GB of RAM.

There are two ways to suspend a virtual machine:

- With a remote console connected to that virtual machine, click **Suspend** on the toolbar.



- With the VMware Management Interface connected to the virtual machine's server, click the pause button (⏸) on the row for that virtual machine.

There are two ways to restore a virtual machine that you have suspended:

- With a remote console connected to that virtual machine, click **Resume** on the toolbar.
- With the VMware Management Interface connected to the virtual machine's server, click the pause button (⏸) on the row for that virtual machine.

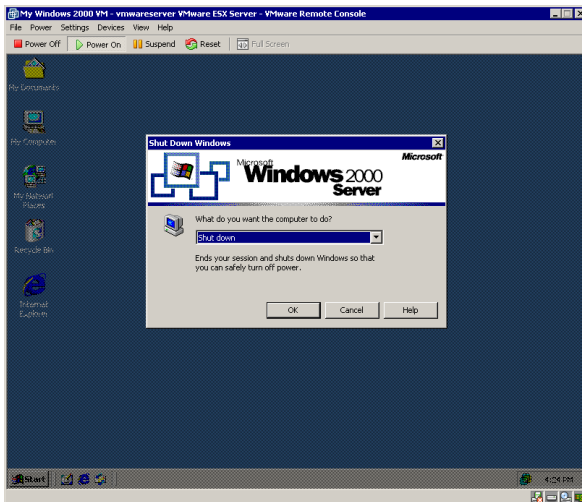
You can also set your virtual machine so it always resumes in the same state. For details, see [Enabling Repeatable Resumes on page 191](#).



### Shutting Down a Virtual Machine

The following steps are based on using a Windows 2000 or Windows NT guest operating system. If you are using a Linux guest operating system, follow the usual steps to shut down the guest operating system inside your virtual machine.

1. Select **Shut Down** from the **Start** menu of the guest operating system (inside the virtual machine).



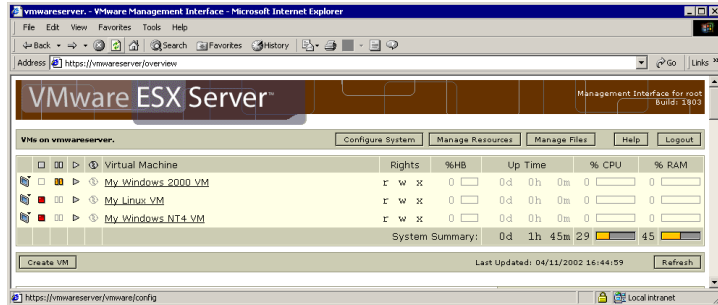
2. Select **Shut Down**, then click **OK**.

## Rebooting or Shutting Down the Server

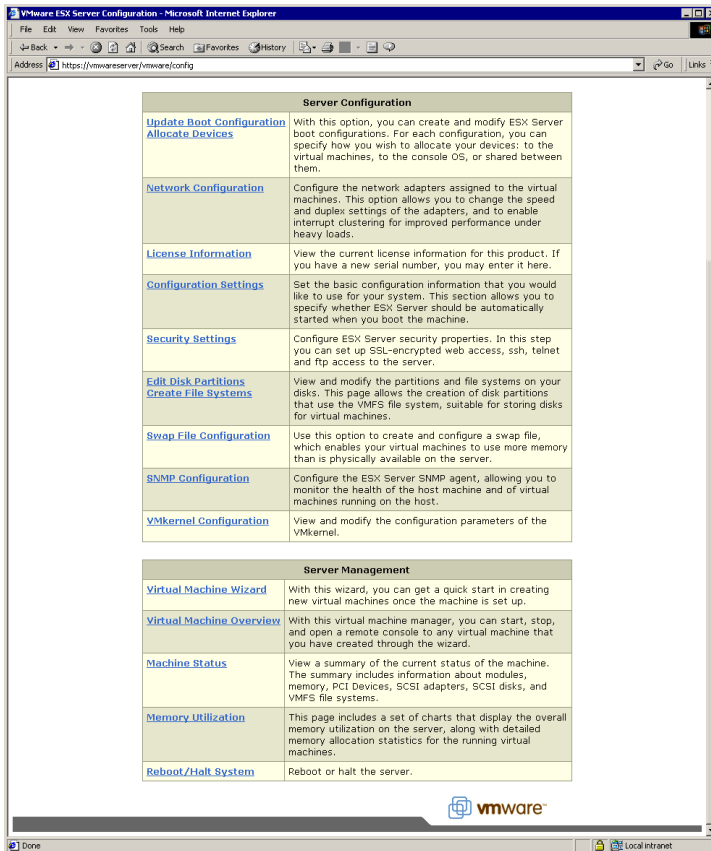
To reboot or shut down the computer where ESX Server is running, take the following steps:

1. Log in to the management interface as root.

The URL to connect to the server is `http://<hostname>/overview/`.

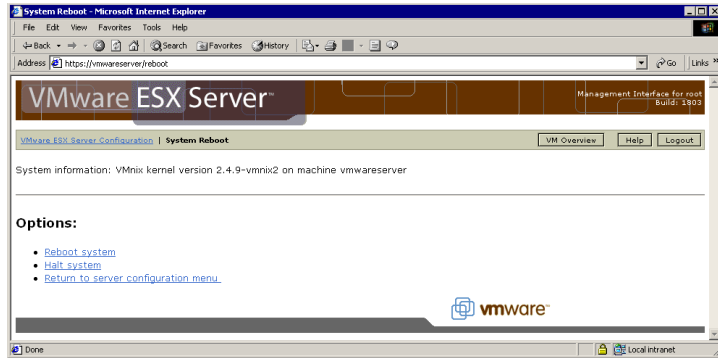


2. At the overview page, be sure all virtual machines are shut down or suspended. Then click **Configure System**.

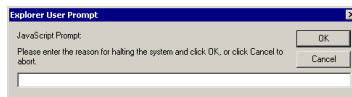


3. Click the **Reboot/Halt System** link.

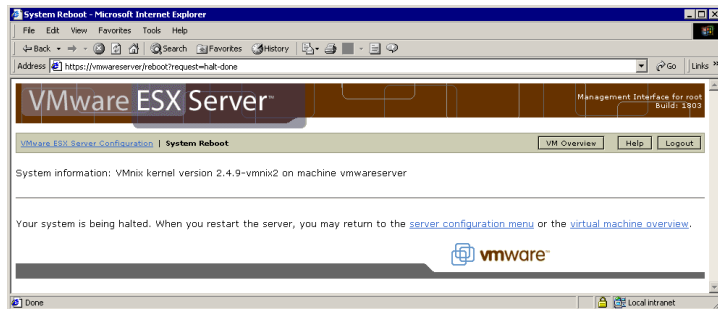
## Running VMware ESX Server



- Click the appropriate link to reboot or halt the system.



- Enter the reason for the reboot or halt. This information is logged for reliability monitoring.



- A confirmation page reports the results of your action.

## Using SNMP with ESX Server

This section contains the following information about using SNMP with ESX Server:

- [Using SNMP to Monitor the Computer Running ESX Server on page 125](#)
  - [Information about the Physical Computer on page 126](#)
  - [Information about the Virtual Machines on page 126](#)
  - [Traps Sent by the Agent on page 127](#)
- [Installing and Running the ESX Server SNMP Agent on page 127](#)
- [Configuring the ESX Server SNMP Agent on page 129](#)
  - [System Information on page 129](#)
  - [Access Control on page 129](#)
  - [Trap Configuration on page 130](#)
  - [Other Configuration File Entries on page 130](#)
  - [Configuration File Issues on page 131](#)
- [Configuring SNMP Management Software on page 131](#)
- [Configuring SNMP Security on page 132](#)
- [Using SNMP with Guest Operating Systems on page 132](#)
- [VMware ESX Server SNMP Variables on page 132](#)

### Using SNMP to Monitor the Computer Running ESX Server

ESX Server ships with an SNMP agent that allows you to monitor the health of the physical machine where ESX Server is running and of virtual machines running on it. This agent is based on Net-SNMP with enhancements to support data specific to ESX Server. Background information on Net-SNMP is available at [net-snmp.sourceforge.net](http://net-snmp.sourceforge.net).

The ESX Server SNMP agent can be used with any management software that can load and compile a management information base (MIB) in SMIV1 format and can understand SNMPv1 trap messages.

To use the ESX Server SNMP agent, configure it following the directions below, then connect to the agent using your management software's normal procedures. The location of the VMware subtree in the SNMP hierarchy is

`.iso.org.dod.internet.private.enterprises.vmware  
(.1.3.6.1.4.1.6876).`

### Information about the Physical Computer

SNMP get variables allow you to monitor a wide variety of items about the physical computer and how virtual machines are using its resources. Some of the key types of information available are:

- The number of CPUs on the physical computer
- CPU resources on the physical computer being used by particular virtual machines
- The amount of RAM installed on the physical computer
- Physical memory used by the console operating system
- Physical memory used by particular virtual machines
- Physical memory that is not being used
- Usage data for disks on the physical computer, including number of reads and writes and amount of data read and written
- Usage data on the physical computer's network adapters, including packets sent and received and kilobytes sent and received
- State of the VMkernel (loaded or not loaded)

**Note:** If the variable showing whether the VMkernel is loaded says no, any values reported for any other variable should be regarded as invalid.

### Information about the Virtual Machines

SNMP get variables allow you to monitor a number of items about particular virtual machines running on the computer. Some of the key types of information available are:

- The path to the virtual machine's configuration file
- The guest operating system running on the virtual machine
- The amount of memory the virtual machine is configured to use
- The state of the virtual machine's power switch — on or off
- The state of the guest operating system — on or off (running or not running)
- What disk adapters are seen by the virtual machine
- What network adapters are seen by the virtual machine
- What floppy disk drives are seen by the virtual machine
- The state of the floppy drive — connected or disconnected
- What CD-ROM drives are seen by the virtual machine

- The state of the CD-ROM drive — connected or disconnected

**Note:** SNMP information is provided for virtual machines if their configuration files are stored locally on the ESX Server computer. If the configuration files are stored on an NFS-mounted drive, information for the virtual machines does not appear in the SNMP tables.

### Traps Sent by the Agent

Four SNMP traps notify you of critical events in particular virtual machines. The affected virtual machine is identified by ID number and configuration file path. The traps notify you

- When a virtual machine is powered on
- When a virtual machine is powered off
- When the virtual machine detects a loss of heartbeat in the guest operating system
- When the virtual machine detects that the guest operating system's heartbeat has started or resumed

**Note:** VMware Tools must be installed in the guest operating system to support the traps that detect loss and resumption of the guest's heartbeat.

**Note:** Traps are not generated immediately when virtual machines are registered using the VMware Management Interface. To enable trap generation, you must restart `vmware-serverd`. You may restart `vmware-serverd` by rebooting the server or by logging in to the console operating system as root and issuing the command

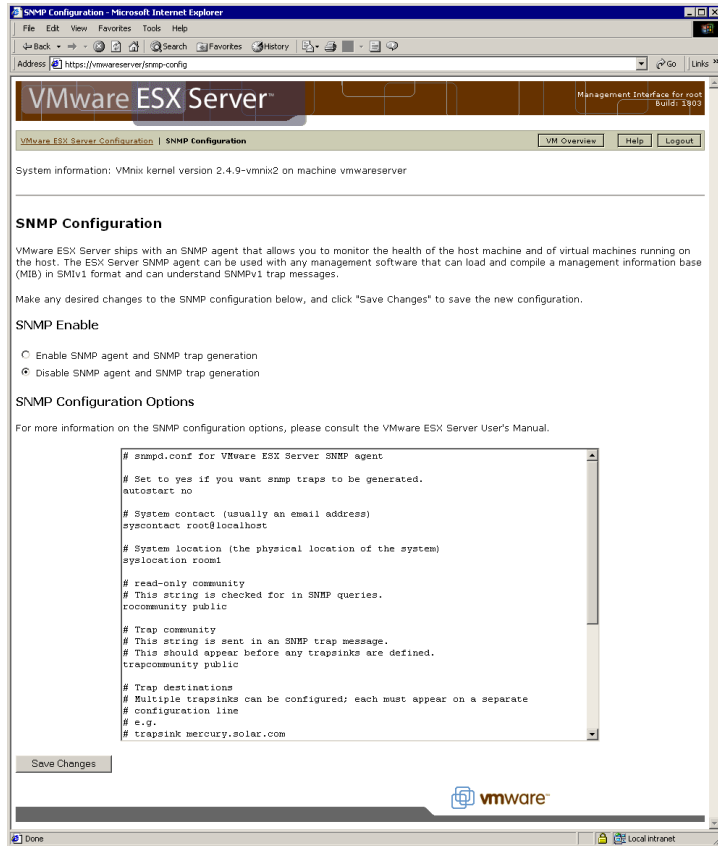
```
killall -HUP vmware-serverd
```

### Installing and Running the ESX Server SNMP Agent

The SNMP agent is installed by default when you install ESX Server. The executables and supporting files are installed in several subdirectories under `/usr`.

The agent is not run by default. To run the agent, set it to start automatically when the system boots using the VMware Management Interface. To do so, follow these steps:

1. Log in to the management interface as root, click **Configure System**, then click **SNMP Configuration**.



2. Select **Enable SNMP agent and SNMP trap generation**.
3. Use the text editor on the page to make any needed changes in the SNMP configuration file. For details, see [Configuring the ESX Server SNMP Agent on page 129](#).
4. Click **Save Changes**.

If you need to start the agent manually, you can do so from the console operating system with this command:

```
snmpd
```



By default, the agent starts and runs as a background process. For details on command line options, see the man page `snmpd(1)`.

### Configuring the ESX Server SNMP Agent

You may configure the SNMP agent from the management interface or from the console operating system in the following ways:

- Use the SNMP configuration page in the management interface to set the agent to start automatically. The SNMP configuration page also includes a text editor you can use to modify the settings in the configuration file.
- Use a text editor on the console operating system to modify the settings in the configuration file, `/usr/share/snmp/snmpd.conf`. The default configuration file is very brief and uses dummy parameters.
- From the console operating system, run the `snmpconf` configuration script to create a new configuration file. This approach is recommended only for users familiar with SNMP. Documentation for the script is provided in the `snmpconf(1)` man page. See the Configuration File Issues section below for restrictions.

The sections that follow describe the default configuration and appropriate settings you can use in each section of the file.

Lines that begin with a `#` symbol are comments in the configuration file.

#### System Information

```
# System contact (usually an email address)
syscontact root@localhost
# System location (the physical location of the system)
syslocation room1
```

The agent uses the information you enter here to provide responses to queries on the `syscontact` and `syslocation` objects in the system sub-tree of the management information base. Replace `root@localhost` and `room1` with values appropriate for your site and the ESX Server computer.

#### Access Control

```
# read-only community
# This string is checked for in SNMP queries.
rocommunity public

# This string is sent in an SNMP trap message.
# This should appear before any trapsinks are defined.
trapcommunity public
```

SNMP uses community names somewhat like passwords. They are exchanged in clear text in communications between the agent and its clients. All requests to the agent must contain a community name, which the agent compares against the one set up in the configuration file to determine what permissions and capabilities the request has.

The VMware SNMP agent sets up a single default read-only community named `public`. This means that, by default, all incoming requests must include `public` as the community name. These read-only requests can only retrieve the values of variables.

The `trapcommunity` parameter is also a community name. This community name is used by the agent. It is included in trap messages that the agent sends.

Give these two parameters values that are appropriate for your site's SNMP management configuration. Remember that the `rocommunity` value must be used when communicating with the agent to get responses, and your management software should expect to see the value of `trapcommunity` in trap messages from the agent.

### Trap Configuration

```
# Trap destinations
# Multiple trapsinks can be configured; each must appear
# on a separate configuration line
# e.g.
# trapsink mercury.solar.com
# trapsink venus.solar.com
trapsink localhost
```

Set the `trapsink` configuration parameter to tell the agent where to send its trap messages. You can configure multiple `trapsink` lines, as indicated in the configuration file's comments. Set the values for this variable to conform to the management structure at your site. For instance, assign the managing workstation's host name as one of the values for this parameter.

### Other Configuration File Entries

```
# VMware ESX Server SNMP modules -- Edit this section at
# your own risk
dlmod SNMPSystem /usr/lib/vmware/SNMPSystem.so
dlmod SNMPVMInfo /usr/lib/vmware/SNMPVMInfo.so
dlmod SNMPVMDisk /usr/lib/vmware/SNMPVMDisk.so
dlmod SNMPVMNet /usr/lib/vmware/SNMPVMNet.so
```

```
dlmod SNMPVMFloppyCD /usr/lib/vmware/SNMPVMFloppyCD.so
dlmod SNMPResCPU /usr/lib/vmware/SNMPResCPU.so
dlmod SNMPResMem /usr/lib/vmware/SNMPResMem.so
dlmod SNMPResDisk /usr/lib/vmware/SNMPResDisk.so
dlmod SNMPResNet /usr/lib/vmware/SNMPResNet.so
```

These parameters, set up by the VMware SNMP package, indicate VMware-specific modules to be loaded. Do not modify the contents of this section.

### Configuration File Issues

Each computer configured to receive traps must be listed separately on its own `trapsink` line, but the community and port options described by the `snmpd.conf` (5) man page are not supported for ESX traps.

The `trap2sink` configuration parameter is ignored by the ESX trap generator, because the ESX Server agent sends SNMPv1 traps. As a result, you should not use this parameter to specify ESX Server trap destinations.

### Configuring SNMP Management Software

To use your SNMP management software with the ESX Server agent, take the normal steps needed to accomplish the following:

- In your management software, specify the ESX Server machine as an SNMP-based managed device.
- Set up appropriate community names in the management software. These must correspond to the values set for `rocommunity` and `trapcommunity` in the ESX Server agent's configuration file.
- Load the ESX Server MIBs into the management software so you can view the symbolic names for the variables. The location of the ESX Server MIBs is `.iso.org.dod.internet.private.enterprises.vmware(.1.3.6.1.4.1.6876)`.

### Preparing for Installation of Compaq Management Agents

Before installing Compaq management agents, log in to the console operating system as root and run the script `/usr/sbin/cmasetup.sh`. This script sets up the environment expected by the installer for the Compaq management agents.

The Compaq cmaX extensions are built into the ESX Server SNMP daemon. After you have run `/usr/sbin/cmasetup.sh`, you may install Compaq agents on the console operating system following the standard instructions.

**Note:** The Compaq agents can see and report on only the devices assigned exclusively to the console operating system. They cannot see and report on devices

that are assigned exclusively to virtual machines or shared between virtual machines and the console operating system.

### Configuring SNMP Security

The ESX Server SNMP package takes the simplest approach to SNMP security. It sets up a single community with read-only access. This is denoted by the `rocommunity` configuration parameter in `snmpd.conf`.

By design, SNMP is not a very secure protocol, and the community-based security model is a retrofit to the protocol.

There are other enhancements to the SNMP security mechanism that allow an administrator to set up a more elaborate permissions scheme. See the `snmpd.conf` (5) man page for details. Note the exceptions mentioned in the Configuration File Issues section above; other settings in the file may be made as described by the man page.

### Using SNMP with Guest Operating Systems

To use SNMP to monitor guest operating systems or applications running in virtual machines, install the SNMP agents you would normally use for that purpose. No special configuration is required.

Keep in mind that the virtual machine uses its own virtual hardware devices. You should not install in the virtual machine agents intended to monitor hardware on the physical computer.

### VMware ESX Server SNMP Variables

The VMware enterprise tree is at `.iso.dod.org.internet.private.enterprises.vmware.(.1.3.6.1.4.1.6876.)`. The tree consists of several groups; the variables in each of the groups are shown in the tables below.

**Note:** All variables are read-only.

The data type field refers to the SNMP type described by the structure of management information (SMI).

**vmware.vmwSystem**

This group consists of three simple variables providing basic information about the system.

Name	Data type	Description
vmwProdName	Display string	Product name.
vmwProdVersion	Display string	Product version.
vmwProdOID	ObjectID	A unique identifier for this product in the VMware MIB. This ID is unique with respect to versions of the same product also.

**vmware.vmwVirtMachines**

This group consists of virtual machine configuration information in six tables.

**vmTable** — index = <vmlidx>, a table containing information on virtual machines that have been configured on the system. Each row provides information about a particular virtual machine.

Name	Data type	Description
vmlidx	Integer	This is a dummy number for an index.
vmDisplayName	Display string	Name by which this virtual machine is displayed.
vmConfigFile	Display string	Path to the configuration file for this virtual machine.
vmGuestOS	Display string	Operating system running on this virtual machine.
vmMemSize	Integer	Memory configured for this virtual machine in MB.
vmState	Display string	Virtual machine on or off.
vmVMID	Integer	If a virtual machine is active, an ID is assigned to it (like a pid). Not all virtual machines may be active, so this cannot be used as the index.
vmGuestState	Display string	Guest operating system on or off.

**hbaTable** — index = <vmlidx, hbaldx>, a table of disk adapters seen by this virtual machine.

Name	Data type	Description
vmlidx	Integer	This number corresponds to the index of the virtual machine in vmTable.
hbaldx	Integer	There is a correspondence to the order of the SCSI device module loaded into the VMkernel.
hbaNum	Display string	Device number ( format: scsi*).
hbaVirtDev	Display string	Virtual device name for this adapter.

**hbaTgtTable** — index = <vmlidx, hbaTgtIdx>, a table of SCSI targets seen by this virtual machine.

Name	Data type	Description
vmlidx	Integer	This number corresponds to the index of the virtual machine in vmTable.
hbaTgtIdx	Integer	This is a dummy target index.
hbaTgtNum	Display string	Target description (format: scsi<hba>:<tgt>).

**netTable** — index = <vmlidx, netIdx>, a table of network adapters seen by this virtual machine.

Name	Data type	Description
vmlidx	Integer	This number corresponds to the index of the virtual machine in vmTable.
netIdx	Integer	Index for this table.
netNum	Display string	Device number. (format: ethernet*)
netName	Display string	Device name of VMkernel device that this virtual network adapter is mapped to. (format: vmnic* or vmnet*)
netConnType	Display string	Connection type (user or virtual machine monitor device).

**floppyTable** — index = <vmldx, flddx>, a table of floppy drives seen by this virtual machine.

Name	Data type	Description
vmldx	Integer	This number corresponds to the index of the virtual machine in vmTable.
flddx	Integer	Index into floppy table. Order of the floppy device on this virtual machine.
fdName	Display string	Device number/name (/dev/fd0, etc. NULL if not present).
fdConnected	Display string	Is the floppy drive connected (mounted)?

**cdromTable** — index = <vmldx, cdromldx>, a table of CD-ROM drives seen by this virtual machine.

Name	Data type	Description
vmldx	Integer	This number corresponds to the index of the virtual machine in vmTable.
cdromldx	Integer	Index into CD-ROM table. Order of the CD-ROM device on this virtual machine.
cdromName	Display string	Device number/name (/dev/CDROM, etc. NULL if not present).
cdromConnected	Display string	Is the CD-ROM drive connected (mounted)?

### vmware.vmwResources

This group contains statistics on the physical machine's resources categorized into several subgroups.

#### vmware.vmwResources.vmwCPU

This group contains CPU-related information in one simple variable and one table.

Name	Data type	Description
numCPUs	Integer	Number of physical CPUs on the system.

**cpuTable** — index = <vmID>, CPU usage by virtual machine.

Name	Data type	Description
vmID	Integer	ID allocated to running virtual machine by the VMkernel.
cpuShares	Integer	Share of CPU allocated to virtual machine by VMkernel.
cpuUtil	Integer	Amount of time the virtual machine has been running on the CPU (seconds).

### vmware.vmwResources.vmwMemory

This group contains RAM information in three simple variables and one table.

Name	Data type	Description
memSize	Integer	Amount of physical memory present on machine (KB).
memCOS	Integer	Amount of physical memory used by the console operating system (KB).
memAvail	Integer	Amount of physical memory available/free (KB).

**memTable** — index = <vmID>, a table of memory usage by virtual machine.

Name	Data type	Description
vmID	Integer	ID allocated to running virtual machine by the VMkernel.
memShares	Integer	Shares of memory allocated to virtual machine by VMkernel.
memConfigured	Integer	Amount of memory the virtual machine was configured with (KB).
memUtil	Integer	Amount of memory utilized by the virtual machine (KB; instantaneous).

### vmware.vmwResources.vmwHBATable

This group contains physical disk adapter and targets information in one table.



**vmwHBATable** — index = <hbaldx>, the disk adapter and target information table.

Name	Data type	Description
hbaldx	Integer	Index into table for HBA (corresponds to the order of the adapter on the physical computer).
hbaName	Display string	String describing the disk. (format: <devname#>:<tgt>:<lun>)
vmID	Integer	ID assigned to running virtual machine by the VMkernel.
diskShares	Integer	Share of disk bandwidth allocated to this virtual machine.
numReads	Integer	Number of reads to this disk since disk module was loaded.
kbRead	Integer	KB read from this disk since disk module was loaded.
numWrites	Integer	Number of writes to this disk since disk module was loaded.
kbWritten	Integer	KB written to this disk since disk module was loaded.

#### vmware.vmwResources.vmwNetTable

This group contains network statistics organized by network adapter and virtual machine, in one table.

**vmwNetTable** — index = <netIdx>, network adapter statistics.

Name	Data type	Description
netIdx	Integer	Index into table for Net (corresponds to the order of the adapter on the physical computer).
netName	Display string	String describing the network adapter (format: vmnic* or vmnet*).
vmID	Integer	ID assigned to running virtual machine by the VMkernel.
ifAddr	Display string	MAC address of virtual machine's virtual network adapter.
netShares	Integer	Share of net bandwidth allocated to this virtual machine. (reserved for future use)
pktsTx	Integer	Number of packets transmitted on this network adapter since network module was loaded.
kbTx	Integer	KB sent from this network adapter since network module was loaded.

Name	Data type	Description
pktsRx	Integer	Number of packets received on this network adapter since network module was loaded.
kbRx	Integer	KB received on this network adapter since system start.

### vmware.vmwProductSpecific

This group contains variables categorized into product-specific subgroups.

### vmware.vmwProductSpecific.vmwESX

This group contains variables specific to VMware ESX Server.

### vmware.vmwProductSpecific.vmwESX.esxVMKernel

This group contains variables specific to VMware ESX Server's VMkernel. It contains one simple variable.

Name	Data type	Description
vmkLoaded	Display string	Has the VMkernel been loaded? (yes/no)

**Note:** If the variable showing the state of the VMkernel says no, any values reported for quantitative variables should be regarded as invalid.

### vmware.vmwTraps

This group contains the variables defined for VMware traps and related variables for use by the trap receiver (for example, `snmptrapd`).

Name	Data type	Description
vmPoweredOn	Trap	This trap is sent when a virtual machine is powered on.
vmPoweredOff	Trap	This trap is sent when a virtual machine is powered off.
vmHBLost	Trap	This trap is sent when a virtual machine detects a loss in guest heartbeat.
vmHBDetected	Trap	This trap is sent when a virtual machine detects or regains the guest heartbeat.
vmID	Integer	This is the vmID of the affected virtual machine in the preceding traps. If the vmID is nonexistent, (such as for a power-off trap) -1 is returned.

Name	Data type	Description
vmConfigFile	Display string	This is the configuration file of the affected virtual machine in the preceding traps.

### **vmware.vmwOID**

There are no variables in this group. This group is used to allocate a unique identifier for the product denoted by the vmwSystem.vmwOID variable.

### **vmware.vmwExperimental**

There are currently no variables in this group. This group is reserved for VMware ephemeral, experimental variables.

## Backing Up Virtual Machines

Your backup strategy depends on how you want to protect your data and recover from problems. There are two main goals.

- Recover individual files on the virtual machine (for example, if a user accidentally removes a file)
- Recover from catastrophic failures in which your entire virtual machine is damaged

VMware ESX Server provides several possible approaches for backing up your data, whether to tape or to another system over the network. You will probably find that a combination of approaches provides the best data protection for your virtual machines.

The next section, [Using Tape Drives with VMware ESX Server](#), describes how to make tape drives available to both your virtual machine and your console operating system:

- [Backing Up from within a Virtual Machine on page 140](#)
- [Backing Up Virtual Machines from the Console Operating System on page 141](#)
- [Using Hardware or Software Disk Snapshots on page 142](#)
- [Using Network-based Replication Tools on page 143](#)

### Using Tape Drives with VMware ESX Server

The management interface allows you to allocate a SCSI controller to the console operating system, to one or more virtual machines or for use by both environments. To make a SCSI tape drive available in a virtual machine, you must allocate the SCSI controller to which it is attached for use only by virtual machines.

You can check the allocation settings for the server's SCSI controllers in the management interface. On the overview page, click **Configure System**. Then on the configuration page, click **Update Boot Configuration/Device Allocation**.

**Caution:** Do not reassign a server's only SCSI controller if the console operating system is running from a drive attached to that controller. If your system is configured this way, you must add a second SCSI controller to control the tape drive.

### Backing Up from within a Virtual Machine

One approach to backing up your data is to back up a particular virtual machine's data just as if it were on a physical machine. To do so, you can run either a direct backup tool or the client component of a client-server backup tool within the virtual machine and configure it for direct access to the network or tape drive.

**Note:** You can also use a virtual machine to run the server component of a client-server backup product, provided you give it access to one or more tape drives.

**Note:** Backing up from within a virtual machine has the benefit of allowing fine-grained recovery of your data.

- You can restore file data by the individual file.
- You can restore database data via the normal database-specific method.

However, if there is a disaster and you need to restore the virtual machine from a backup made from within the virtual machine, you need to recreate the virtual machine and load recovery software into it before restoring data from the backups.

To configure a virtual machine so you can use a tape drive from within it, follow these steps:

1. Be sure the virtual machine is powered off so you can modify the configuration.
2. Check the configuration page in the management interface to be sure the controller to which the tape drive is attached is allocated for the exclusive use of virtual machines.
3. Return to the overview page, move the mouse pointer over the terminal icon beside the name of the virtual machine on which you want to use the tape drive, then choose **Edit Configuration**.
4. In the SCSI Devices section of the configuration page, click the check box to select the virtual SCSI device you want to connect to the tape drive. Click **New Disk...**, then from the drop-down list on the Create VMFS File page, choose the device name that has the word `tape` in parentheses next to it. For example, if the tape device is on the server's second SCSI controller at target ID 0 and LUN 0, the device name might be `vmhba1 : 0 : 0 : 0 (tape)`. The partition number for a tape drive is always 0.
5. Click **Create**. Then on the Configure VM page, click **Save Changes** to save the updated configuration.
6. Power on the virtual machine. The tape drive should be available at the SCSI ID you selected on the virtual machine's configuration page.

## Backing Up Virtual Machines from the Console Operating System

You may also choose to back up your virtual machines by copying to tape the entire virtual disk files and any redo logs, along with the backups of the console operating system. This approach has the benefit of making it easy to restore your virtual

machines in the event of a full system loss or data loss due to failure of unprotected disks.

However, these full-image backups do not permit you to restore individual files. You must restore the entire disk image and any associated logs, then power on a virtual machine with these drives connected to retrieve specific data.

The next section describes how to ensure data integrity when backing up virtual machines from the physical computer or the console operating system.

### **Providing Optimum Data Integrity In Virtual Machine Backups Without Downtime**

You can use the Perl API included with ESX Server 1.5 in conjunction with backup products to provide snapshots, or stable disk or redo log images. The appropriate functions can be called from within many backup products in order to establish a safe basis for backing up images or logs. You may use this approach with any disk mode — persistent, undoable, nonpersistent or append.

To add a new redo log to a disk image while a virtual machine is running, a Perl program would use a call of the format:

```
$vm->add_redo( $disk )
```

Once this call completes, new writes go into the new log file, making the underlying disk image or redo log a stable, read-only file that you can copy to another location on disk, directly to tape, or to another network location.

When you finish copying the files, you can commit the changes in the new log to the original disk or redo log:

```
$vm->commit( $disk, $level, $freeze, $wait )
```

For incremental disk-level backups, add a redo log on top of the current log, back up the underlying log and commit the new log. You can apply the most recent day's saved redo log to the full backup's complete disk image.

For additional information on the Perl API, see the VMware Perl API documentation at [www.vmware.com/support/developer/perl-API/doc/](http://www.vmware.com/support/developer/perl-API/doc/).

### **Using Hardware or Software Disk Snapshots**

You may choose to use the snapshot capabilities offered by your disk subsystem, file system or volume manager to provide stable copies of disk images. As with physical servers, consider using some level of application integration so you can be sure your backups have the desired level of data integrity.

You can combine these approaches with the ESX Server redo log API (described in [Providing Optimum Data Integrity In Virtual Machine Backups Without Downtime on page 142](#)) to keep the interval during which an extra log is used to a minimum. To do this, take the following general steps:

- Add the new redo log.
- Take a snapshot of the mirror using your disk subsystem's or volume manager's interfaces.
- Commit the changes to the live log.

You may still back up from the stable disk image on the snapped mirror, then reconnect the mirror to have it pick up the latest changes in time for your next backup.

### Using Network-based Replication Tools

Many enterprise disk storage subsystems can be configured to replicate, or mirror, their data to another subsystem at a local or remote location. This replication can occur either synchronously or asynchronously.

- If the replication is synchronous, a write operation does not appear to be completed locally until the data is committed to disk at the remote location.
- This improves data integrity but presents a potential performance bottleneck.
- If the replication is asynchronous, the remote copy is permitted to be some number of write operations behind the most current local data.

This accepts a higher potential of inconsistent data at the remote site in exchange for increased performance.

Either of these hardware-based approaches may be used with ESX Server.

In addition, some disaster protection software products implement remote mirroring in software. These tools provide protection and data integrity semantics similar to those of the hardware-based solutions. However, they may be more cost-effective for configurations with low to medium performance requirements.

These software tools can be used inside guest operating systems.

**Note:** We recommend that you do not use software remote mirroring tools for console operating system-driven replication on VMware ESX Server. This is because these software tools usually require file system format awareness, add significantly to the network I/O level and the CPU requirements to service that network I/O, and are more common on Windows and Unix operating systems than on Linux.

## The VMware Guest Operating System Service

When you install VMware Tools in a virtual machine, the VMware guest operating system service is one of the primary components installed. The guest service can do the following:

- Execute commands in the virtual machine when it is requested to halt or reboot the guest operating system.
- Gracefully power off and reset a virtual machine.
- Send a heartbeat to VMware ESX Server so that it knows the guest operating system is running.
- Synchronize the time of the guest operating system with the time on the physical computer.
- Pass a string from the console operating system to the guest operating system.

The guest service starts automatically when you boot the guest operating system.

In a Linux guest, the guest service is called `vmware-guestd`. To display help about the guest service, including a list of all options, use the following command:

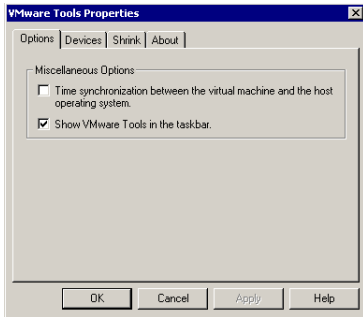
```
/etc/vmware/vmware-guestd --help
```

In a Windows guest, the guest service program file is called `VMwareService.exe`. To display help, right-click the VMware Tools icon in the system tray and choose **Help**.

### Synchronizing the Time Between the Guest and Console Operating Systems

The guest service can synchronize the date and time between the guest and console operating systems once every second. In the VMware Tools control panel, on the Other tab (Options in a Linux guest), select **Time synchronization between the virtual machine and the host operating system**.





In addition, the guest service can synchronize the date and time between the guest and console operating systems in response to various system events — for example, when you resume from disk. You can disable this in the configuration file by setting

```
time.synchronize.resume.disk = FALSE
```




### Shutting Down and Restarting a Virtual Machine

ESX Server can signal the guest service to shut down or restart a virtual machine. After the guest service receives a request to shut down or restart, it sends an acknowledgment back to ESX Server.

You can send these requests from the VMware Management Interface or the console operating system's command line.

Whether it is possible to shut down or restart a virtual machine depends on the state of the virtual machine.

#### Shutting Down or Restarting a Virtual Machine from the VMware Management Interface

You can click  to shut down or  to restart a virtual machine from the VMware Management Interface. These operations are also available from the menu that appears when you hold your mouse over the terminal icon (). After you select one of these operations, you should click to the Event Log page for this virtual machine to respond to any messages that require a response.

Shutting down is the equivalent of using the guest operating system's shut down command, then turning off power to the virtual machine. Restarting is the equivalent of using the guest operating system's restart command.

If you receive an event log message saying, "You will need to power off or reset the virtual machine at this point," you must connect to the virtual machine with a remote console and click **Power Off** or **Reset** to complete the operation.

The power off and reset commands are not available while these operations are in progress.

You can also force power off or force reset from the menu. These commands bypass the guest service and perform the virtual equivalent of shutting off the power to a physical machine or pressing a physical reset button.

### Shutting down or Restarting a Virtual Machine from the Command Line

You can shut down and restart a virtual machine from the console operating system command line using the `vmware-control` program.

The following commands return you to the command prompt immediately, before they finish executing, although the shut down or restart process may take some time to complete:

```
vmware-control /<path_to_config_file>/<configfile>.cfg \  
request_stop  
  
vmware-control /<path_to_config_file>/<configfile>.cfg \  
request_reset
```

**Note:** Enter the `vmware-control` command you want to use on a single line. Do not type the backslash.

### Executing Commands When ESX Server Requests the Guest Service to Halt or Reboot a Virtual Machine

In a Linux guest, you can have the guest service execute specific commands when ESX Server asks it to halt or reboot the virtual machine's guest operating system. If you use nonstandard utilities or want to do additional things before shutting down or rebooting the guest operating system, you can override the default commands the guest service executes by modifying the `/etc/vmware/dualconf.vm` startup script in the guest to start the guest service with the following command line options:

```
/etc/vmware/vmware-guestd --halt-command <command>
```

where `<command>` is the command to execute when ESX Server asks the guest service to halt the guest operating system

```
/etc/vmware/vmware-guestd --reboot-command <command>
```

where `<command>` is the command to execute when ESX Server asks the guest service to reboot the guest operating system

## Passing a String from the Console Operating System to the Guest Operating System

With ESX Server and knowledge of a scripting language like Perl or NetShell (in a Windows 2000 guest operating system), you can pass a string from your virtual machine's configuration file to the guest operating system when you use the configuration file to launch a virtual machine. This string is known as `machine.id`. The content of the string you pass to the guest operating system is up to you.

For additional details and sample scripts, including information on passing messages both ways between the console operating system and a guest, see the VMware Perl API documentation at [www.vmware.com/support/developer/perl-API/doc/](http://www.vmware.com/support/developer/perl-API/doc/).

You should use this feature only if you have a good understanding of a scripting language and know how to modify system startup scripts.

### Example of Passing a String from the Console Operating System to the Guest

If you use multiple configuration files that point to the same virtual disk, each configuration file can contain its own unique `machine.id` line.

`<config_file_1>.cfg` contains:

```
scsi0:1.present = TRUE
scsi0:1.name = "my_common_virtual_hard_drive.dsk"
scsi0:1.mode = "persistent"
machine.id = "the_id_for_my_first_vm"
```

`<config_file_2>.cfg` contains:

```
scsi0:1.present = TRUE
scsi0:1.name = "my_common_virtual_hard_drive.dsk"
scsi0:1.mode = "persistent"
machine.id = "the_id_for_my_second_vm"
```

Using `machine.id`, you may pass such strings as the Windows system ID (SID), a machine name or an IP address. In the guest operating system startup script, you may then have the guest service retrieve this string, which can then be used by your script to set your virtual machine's system ID, machine name or IP address.

In the following example, we use a Linux guest to illustrate how you can use the guest service to retrieve a string containing what becomes the virtual machine's machine name and IP address. We use RedHat62VM as the machine name and 148.30.16.24 as the IP address.

1. Define the `machine.id` string. Add the following line to your virtual machine's configuration file:  
`machine.id = "RedHat62VM 148.30.16.24"`

Then launch a virtual machine using this configuration file.

2. Retrieve the `machine.id` string in the virtual machine. In your system startup script, before the network startup section, add the following command:  
`/etc/vmware/vmware-guestd --cmd 'machine.id.get'`

**Note:** in a Windows guest, the command to retrieve the string is  
`VMwareService --cmd machine.id.get`

You need to further customize this startup script so it uses the string the guest service retrieved during startup to set the virtual machine's network name to RedHat62VM and its IP address to 148.30.16.24. This should be located in the script before the network services are started. If you're using a Windows 2000 guest operating system, for example, you can call the NetShell utility (`netsh`) and pass it the contents of the string, which it can then use appropriately (that is, it can set a new IP address for the virtual machine, if that is what was passed in the string originally).

From the console operating system, you can prevent the console operating system from passing a string to the guest operating system via the guest service. To do this, set the following line in your virtual machine's configuration file.

```
isolation.tools.machine.id.get.disable = TRUE
```

# 4

## **Guest Operating Systems**

## Guest Operating Systems

This section provides information on the following:

- [Installing Guest Operating Systems on page 151](#)
- [The VMware Guest Operating System Service on page 167](#)

# Installing Guest Operating Systems

Guest operating system installation instructions assume you are using a remote console on a management workstation with a network connection to the server that hosts your virtual machine. If you are installing the guest operating system from CD-ROM discs or floppy disks, you need access to the server so you can insert the media into the appropriate drives.

If you prefer to install over a network, you need ISO image files of installation CD-ROMs and floppy image files of any floppy disks needed for the installation. The installation instructions in this section assume you are installing from physical media. If you are using image files, you should connect the virtual machine's CD-ROM or floppy drives to the appropriate image files before you begin installing the guest operating system.

For an overview of the guest operating system installation process, see [Installing a Guest Operating System and VMware Tools on page 70](#).

The following sections describe specific guest operating systems:

- [Windows 2000 Installation Guidelines on page 152](#)
- [Windows NT Installation Guidelines on page 153](#)
- [Red Hat Linux 7.3 Installation Guidelines on page 154](#)
- [Red Hat Linux 7.1 and 7.2 Installation Guidelines on page 156](#)
- [Red Hat Linux 7.0 Installation Guidelines on page 158](#)
- [Red Hat Linux 6.2 Installation Guidelines on page 160](#)
- [SuSE Linux 7.3 Installation Guidelines on page 162](#)
- [FreeBSD 4.5 Installation Guidelines on page 164](#)

### Windows 2000 Installation Guidelines

Windows 2000 server versions can be installed in a virtual machine using the corresponding Windows 2000 distribution CD. Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

**Note:** Some Microsoft Windows 2000 disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 2000 operating system on your actual computer, you may not be able to install it in a VMware ESX Server virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

### Windows 2000 Installation Steps

1. Before starting the installation, use the VMware Management Interface to verify the virtual machine's devices are set up as you expect. For example, if you would like networking software to be installed during the Windows 2000 installation, be sure the virtual machine's Ethernet adapter is configured and enabled.

If you plan to install the guest operating system from a physical CD-ROM disc, be sure the CD-ROM drive is connected to the virtual machine.

2. Insert the Windows 2000 CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows 2000.
4. If you enabled the virtual machine's Ethernet adapter and selected the `v1ance` driver, a VMware PCI Ethernet Adapter is detected and set up automatically.

If you enabled the virtual machine's Ethernet adapter and selected the `vmxnet` driver, you need to configure the guest operating system's network adapter when you install VMware Tools.

### VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

**Note:** After you install VMware Tools, you need to change your Windows 2000 screen area to be greater than 640x480 pixels; otherwise, Windows 2000 uses the standard VGA driver and your performance suffers.



### Windows NT Installation Guidelines

Windows NT 4.0 can be installed in a virtual machine using the standard Windows NT CD. Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

**Note:** Windows NT 4.0 virtual machines must have Service Pack 4 or higher installed. If your initial installation is from an installation disc that has a lower service pack level, first create the virtual machine with 2GB of RAM or less. After applying Service Pack 4 or higher, you may use the VMware Management Interface to increase the memory setting to as much as 3.6GB.

### Windows NT Installation Steps

1. Use the VMware Management Interface to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Windows NT installation, be sure the virtual machine's Ethernet adapter is configured and enabled.

If you plan to install the guest operating system from a physical CD-ROM disc, be sure the CD-ROM drive is connected to the virtual machine.

2. Insert the Windows NT CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows NT.
4. If you have enabled the virtual machine's Ethernet Adapter, a VMware PCI Ethernet Adapter is detected and set up automatically. The default settings should work fine and do not need to be changed.
5. Finish the Windows NT installation.

### VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

### Red Hat Linux 7.3 Installation Guidelines

The easiest method of installing Red Hat Linux 7.3 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.3 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

**Note:** You should not run the X server that is installed when you set up Red Hat Linux 7.3. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.3.

#### Installation Steps

1. Use the VMware Management Interface to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.3 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.3 CD-ROM in the CD-ROM drive and power on the virtual machine.

You need to install Red Hat Linux 7.3 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.3 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...  
To install or upgrade a system ... in text mode, type: text <ENTER>.  
To enable expert mode, ...  
Use the function keys listed below ...  
To choose the text mode installer, type text followed by Enter.
```

3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons?** option for three-button mouse support in the virtual machine.
5. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.

6. In the Package Group Selection screen, select **Software Development**. If you select **Select individual packages**, be sure to include the gcc compiler. You will need it during installation of VMware Tools.
7. You may see a warning that says:  
`Bad partition table. The partition table on device sda is corrupted. To create new partitions, it must be initialized, causing the loss of ALL DATA on the drive.`  
This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.
8. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen.
9. If your host operating system supports DHCP and is connected to a LAN, then in the Network Configuration screen, select the **Use bootp/dhcp** option.
10. In the Video Card Selection screen, choose any card from the list.
11. In the Video Card Configuration screen, choose **Skip X Configuration**.
12. Log in to the Red Hat 7.3 guest operating system as root and add a symbolic link that is needed for successful installation of VMWare Tools.

```
ln -s /usr/src/linux2.4 /usr/src/linux
```

13. This completes basic installation of the Red Hat Linux 7.3 guest operating system. Be sure to install VMware Tools in your virtual machine. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

**Note:** With a Red Hat Linux 7.3 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

### Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

### Red Hat Linux 7.1 and 7.2 Installation Guidelines

The easiest method of installing Red Hat Linux 7.1 or 7.2 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.1 or 7.2 via the boot floppy/network method is supported as well. Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

Install Red Hat Linux 7.1 or 7.2 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.1 or 7.2 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...  
To install or upgrade a system ... in text mode, type: text <ENTER>.  
To enable expert mode, ...  
Use the function keys listed below ...
```

To choose the text mode installer, type `text` followed by Enter.

**Note:** You should not run the X server that is installed when you set up Red Hat 7.1 or 7.2. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat 7.1 or 7.2.

### Red Hat Linux 7.1 or 7.2 Installation Steps

1. Use the VMware Management Interface to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.1 or 7.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured.

If you plan to install the guest operating system from a physical CD-ROM disc, be sure the CD-ROM drive is connected to the virtual machine.

2. Insert the Red Hat Linux 7.1 or 7.2 CD in the CD-ROM drive and click the **Power On** button. The virtual machine should start booting from the CD and the installation process will begin.

You may see a warning message that says: "Bad partition table. The partition table on device hda is corrupted." This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Initialize** button and press Enter.

3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In Video Card Selection choose **Generic VGA compatible**, then click **OK**.
5. Near the end of the installation, after files have been copied, you reach the Monitor Setup screen. Choose **Generic Standard VGA, 640x480 @ 60 Hz**, then click **OK**.
6. At the Video Memory screen, choose **256KB**, then click **OK**.
7. At the Clockchip Configuration screen, choose **No Clockchip Setting (recommended)**, which is the default, then click **OK**.
8. At the Probe for Clocks screen, click **Skip**.
9. At the Select Video Modes screen, don't choose anything. Just click **OK**.
10. At the Starting X screen, click **Skip**.
11. This completes basic installation of the Red Hat Linux 7.1 or 7.2 guest operating system. Be sure to install VMware Tools in your virtual machine. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

**Note:** With a Red Hat Linux 7.1 or 7.2 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

### Red Hat Linux 7.0 Installation Guidelines

The easiest method of installing Red Hat Linux 7.0 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.0 via the boot floppy/network method is supported as well. Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

Install Red Hat Linux 7.0 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.0 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...  
To install or upgrade a system ... in text mode, type: text <ENTER>.  
To enable expert mode, ...  
Use the function keys listed below ...
```

Choose the text mode installer by typing `text` followed by Enter.

**Note:** During the Red Hat Linux 7.0 text mode installation, a standard XFree86 version 4 server (without support for VMware SVGA or standard VGA) is installed. Do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.0.

### Red Hat Linux 7.0 Installation Steps

1. Use the VMware Management Interface to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured.

If you plan to install the guest operating system from a physical CD-ROM disc, be sure the CD-ROM drive is connected to the virtual machine.

2. Insert the Red Hat Linux 7.0 CD in the CD-ROM drive and click the **Power On** button. The virtual machine should start booting from the CD and the installation process begins.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In Video Card Selection choose **Generic VGA compatible**, then click **OK**.

5. Near the end of the installation, after files have been copied, you reach the Monitor Setup screen. Choose **Generic Standard VGA, 640x480 @ 60 Hz**, then click **OK**.
6. At the Video Memory screen, choose **256Kb**, then click **OK**.
7. At the Clockchip Configuration screen, choose **No Clockchip Setting (recommended)**, which is the default, then click **OK**.
8. At the Probe for Clocks screen, click **Skip**.
9. At the Select Video Modes screen, don't choose anything. Just click **OK**.
10. At the Starting X screen, click **Skip**.

**Note:** This is the most important step. Clicking **OK** runs the XFree86 version 4 server, which fails, and the installer aborts.

11. This completes basic installation of the Red Hat Linux 7.0 guest operating system.

**Note:** We have occasionally observed an error message at the end of the Red Hat 7.0 installation process — one that sounds serious but does not, in fact, indicate a problem.

After your Red Hat 7.0 installation is completed and you click **OK** in the final dialog to reboot the machine, you might see this message as the machine is being shut down.

```
Install exited abnormally -- received signal 11
```

However, the Red Hat 7.0 installation has completed successfully, and the operating system boots with no problems when you restart the virtual machine.

### VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

**Note:** With a Red Hat Linux 7.0 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

### Red Hat Linux 6.2 Installation Guidelines

The easiest method of installing Red Hat Linux 6.2 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 6.2 via the boot floppy/network method is supported as well. Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

**Caution:** Red Hat Linux 6.2 does not run on Pentium 4 processors. It also does not run on Xeon processors that are branded Xeon, with no qualifier, or Xeon-MP (Pentium III Xeon processors are OK).

Install Red Hat Linux 6.2 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 6.2 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...  
To install or upgrade a system ... in text mode, type: text <ENTER>.  
To enable expert mode, ...  
Use the function keys listed below ...
```

Choose the text mode installer by typing `text` followed by Enter.

**Note:** During the Red Hat Linux 6.2 installation, a standard VGA16 X server (without support for the VMware ESX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 6.2.

### Red Hat Linux 6.2 Installation Steps

1. Use the VMware Management Interface to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 6.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured.

If you plan to install the guest operating system from a physical CD-ROM disc, be sure the CD-ROM drive is connected to the virtual machine.

2. Insert the Red Hat Linux 6.2 CD in the CD-ROM drive and click the **Power On** button. The virtual machine should start booting from the CD and the installation process begins.
3. Follow the installation steps as you would for a real PC.



**Note:** If the virtual machine's Ethernet adapter has been enabled, the installation program automatically detects and loads the AMD PC/Net 32 driver (no command line parameter is necessary to load the driver).

4. During the Linux installation, select the standard VGA16 X server. Select the **Generic VGA compatible/Generic VGA** card from the list in the Choose a Card screen. Select the **Generic Monitor** entry from the list in the Monitor Setup screen. Select the **Probe** button from the Screen Configuration dialog and select **OK** from the Starting X dialog.

After you finish installing Linux, Be sure to install VMware Tools in your guest operating system. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#). When you install VMware Tools, the generic X server is replaced with the accelerated X server included in the VMware Tools package.

5. Finish installing Red Hat Linux 6.2 as you would on a physical machine.  
At this point Red Hat 6.2 boots and presents a login screen.

### SuSE Linux 7.3 Installation Guidelines

The easiest method of installing SuSE Linux 7.3 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.3 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have created a new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

**Note:** Note: You should not run the X server that is installed when you set up SuSE 7.3. Instead, to get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.3.

### SuSE Linux 7.3 Installation Steps

1. Use the VMware Management Interface to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.3 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured.

If you plan to install the guest operating system from a physical CD-ROM disc, be sure the CD-ROM drive is connected to the virtual machine.

2. Insert the SuSE Linux 7.3 installation CD in the CD-ROM drive and click the Power On button. The virtual machine should start booting from the CD and the installation process begins.

Installation is faster with the text-mode installer. Press F2 to select it.

3. Follow the installation steps as you would for a physical machine
4. Part way through the installation, the installer reboots the virtual machine.
5. At the Desktop Settings screen, select 640x480 256 colors. After you install VMware Tools in a later step, you can change your screen resolution and number of colors to any settings you wish.
6. At the Configure Monitor screen, choose any monitor. You must choose some monitor so the installer will install a required package.
7. At the Desktop Settings screen, select **Text mode only**.
8. Finish installing SuSE Linux 7.3 as you would on a physical machine. At the end of the installation, boot again using the default LILO selection of `linux`.
9. Log in to the guest operating system as root.

10. Run YaST to configure networking in the guest.

```
yast
```

11. Run SaX2 and configure X to set the screen resolution and color depth you prefer.

```
sax2
```

**Note:** You must run SaX2 on the Linux console, not on X, to make these settings.

12. Reboot your SuSE Linux 7.3 virtual machine. Networking and X should function correctly.

### FreeBSD 4.5 Installation Guidelines

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the ESX Server Virtual Machine Wizard.

When selecting installation options, be sure to install the kernel source code. It is needed during installation of VMware Tools.

The Linux emulation support in FreeBSD is insufficient to run the X server provided by VMware for use on Linux systems running in a virtual machine. The VGA server distributed with FreeBSD works as expected.

The generic FreeBSD kernel works well.

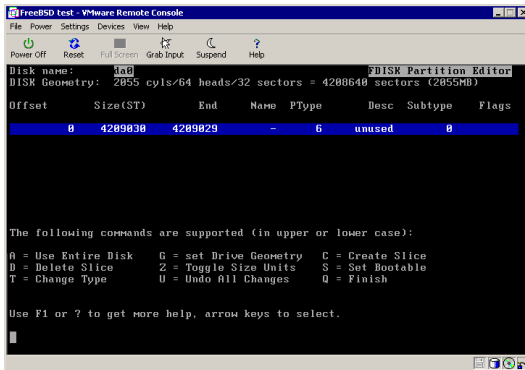
**Note:** FreeBSD has a problem probing for the CD-ROM device `wcd1`. FreeBSD sends an illegal ATAPI command to the IDE controller and ignores the error status reply. This results in a delay of approximately one minute each time the system boots.

### Setting the Disk Geometry for a FreeBSD SCSI Virtual Disk

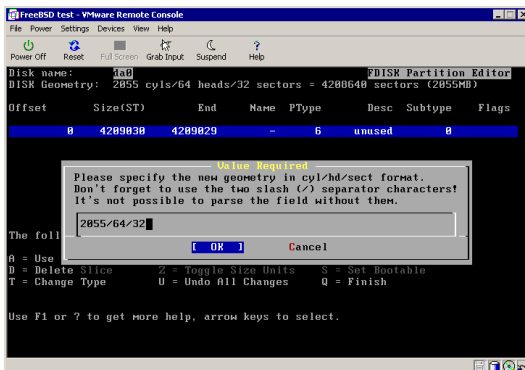
If you are running a virtual machine with FreeBSD 4.5 as the guest operating system on a 2GB or larger SCSI virtual disk, the guest operating system does not boot.

It fails to boot because the virtual disk geometry is not probed correctly by FreeBSD 4.5 when you install the guest operating system. FreeBSD 4.5 installs the boot loader in the wrong location on the virtual disk. When FreeBSD tries to boot, the FreeBSD boot loader asks the BIOS for important data that is now on a different section of the virtual disk, so FreeBSD cannot boot.

To use FreeBSD 4.5 in your virtual machine, you can set the disk geometry by hand when installing FreeBSD. To set the disk geometry manually, complete these steps.



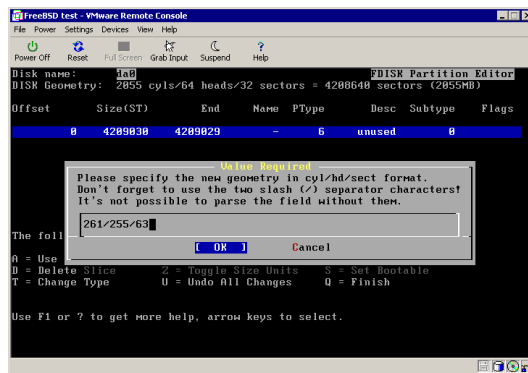
1. FreeBSD calculates an incorrect disk geometry before you arrive at the FDISK Partition Editor, as illustrated here.



2. To set the disk geometry, press G to select the Set Drive Geometry option. A dialog box appears, containing numbers like 2055/64/32, representing the incorrect geometry in cylinders, heads and sectors per head.
3. To calculate the correct geometry, find the total number of sectors by multiplying the number of cylinders, heads and sectors per head together, then dividing the number of sectors by the correct number of heads and sectors per head.

In the above illustration, the virtual disk is a 2055MB disk with 2055 cylinders, 64 heads and 32 sectors per head (these numbers represent the incorrect geometry). The product of these three numbers (2055 x 64 x 32) equals 4,208,640 sectors.

To determine the correct geometry for the BusLogic compatible virtual SCSI adapter used by ESX Server, calculate the number of cylinders, which is 4,208,640 sectors divided by the product of the actual number of heads and sectors per head (255 heads times 63 sectors per head). This results in a total of 261 actual cylinders ( $4208640 / (255 * 63) = 261$ , rounded down).



4. You can now enter the correct geometry of 261 cylinders, 255 heads and 63 sectors per head by typing 261/255/63 in the dialog box. Then click **OK** and continue installing FreeBSD.

### VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

# The VMware Guest Operating System Service

When you install VMware Tools in a virtual machine, the VMware guest operating system service is one of the primary components installed. The guest service can do the following:

- Execute commands in the virtual machine when it is requested to halt or reboot the guest operating system.
- Gracefully power off and reset a virtual machine.
- Send a heartbeat to ESX Server so that it knows the guest operating system is running.
- Synchronize the time of the guest operating system with the time in the console operating system.
- Pass a string from the console operating system to the guest operating system.

The guest service starts automatically when you boot the guest operating system.

In a Windows guest, the guest service program file is called `VMwareService.exe`. For help information, right-click the VMware Tools icon in the system tray and choose Help.

In a Linux guest, the guest service is called `vmware-guestd`. To display help about the guest service, including a list of all options, use the following command:

```
/etc/vmware/vmware-guestd --help
```





# 5

## **Console Operating System and VMkernel**

# Console Operating System and VMkernel

The following sections provide reference information about the console operating system and VMkernel:

- [Characteristics of the VMware Console Operating System on page 171](#)
  - [Using DHCP for the Console Operating System on page 171](#)
- [Loading and Unloading the VMkernel on page 173](#)
  - [The VMkernel Loader on page 173](#)
  - [Example Uses of vmkloader on page 173](#)
- [Configuring Your Server to Use VMkernel Device Modules on page 174](#)
  - [Loading VMkernel Device Modules on page 174](#)
  - [VMkernel Module Loader on page 174](#)
  - [Other Information about VMkernel Modules on page 177](#)

# Characteristics of the VMware Console Operating System

The purpose of the VMware Console Operating System is to start up and administer your virtual machines. It is a customized version of Linux based on the Red Hat 7.2 distribution. It has been modified so it can be managed by the VMkernel.

The console operating system has been customized to disable unneeded services. In particular, most network services have been disabled, except for auth. For remote access to the console operating system, ssh is enabled by default. The root user can modify settings for ssh, Telnet and FTP using the security configuration page in the management interface (<http://<servername>/security-config>).

The console operating system is scheduled by the VMkernel just as any other virtual machine is. You should not attempt to run heavy workloads on the console operating system, because it takes processor cycles away from your virtual machines.

You should also avoid running X on the console operating system. However, if you do choose to run X and the GNOME desktop, remember to disable any GNOME applications that automount the CD-ROM, such as `magicdev`. Otherwise the CD-ROM is not available to the guest operating systems. You can either use the command `killall magicdev` or edit `.gnome/magicdev` and add the following line:

```
do_automount=false, do_cd_play=false
```

RPM installers for the Netscape Communicator 4.78 and Mozilla Web browsers are included on the ESX Server CD-ROM. However, these browsers are not installed by default.

## Using DHCP for the Console Operating System

The recommended setup is to use static IP addresses for the console operating system. It is also possible to set up the console operating system to use DHCP, so long as your DNS server is capable of mapping the console operating system's host name to the dynamically-generated IP address.

If your DNS server cannot map the host's name to its DHCP-generated IP address, which may be the case, you must determine the console operating system's numeric IP address yourself and use that numeric address when accessing the management interface's Web pages.

Keep in mind that the numeric IP address may change as DHCP leases run out or when the system is rebooted. For this reason, we do not recommend using DHCP for

the console operating system unless your DNS server can handle the host name translation.

# Loading and Unloading the VMkernel

## The VMkernel Loader

The program `vmkloader` loads or unloads the VMkernel. With no flags, it loads the VMkernel specified by `<vmkernel-binary>`. If the VMkernel is already loaded, the load fails.

If the unload option (`-u`) is specified, the `<vmkernel-binary>` argument is ignored and the VMkernel is unloaded as long as no virtual machines are currently running on the VMkernel. If there are virtual machines running, then the unload fails. If the force option is specified (`-f`), `vmkloader` unloads the VMkernel even if there is a virtual machine running.

If you have a SCSI adapter or RAID controller shared between the console operating system and the virtual machines, you cannot unload the VMkernel.

### Options

`-f`

Unload the VMkernel even if a virtual machine is currently running on it.

`-n <num>`

Force the VMkernel and all virtual machines to run on only `<num>` processors, even if the physical machine has more than `<num>` processors.

`-s`

Force the VMkernel and all virtual machines to run on only a single processor, even if the physical machine is a multiprocessor computer. This is the same as specifying the option `-n 1`.

`-u`

Unload the VMkernel

### Example Uses of `vmkloader`

The following are some example uses of `vmkloader`.

```
vmkloader /usr/lib/vmware/vmkernel
```

loads the VMkernel binary `/usr/lib/vmware/vmkernel`.

```
vmkloader -u
```

unloads the VMkernel if there are no virtual machines running.

```
vmkloader -uf
```

unloads the VMkernel even if there are virtual machines running.

# Configuring Your Server to Use VMkernel Device Modules

## Loading VMkernel Device Modules

The installation process should detect the devices that are assigned to the VMkernel and automatically load appropriate modules into the VMkernel to make use of these devices.

However, there may be situations in which you wish to load VMkernel device modules explicitly. Modules supported in this release are located in `/usr/lib/vmware/vmkmod`. The command `vmkload_mod(1)` loads VMkernel modules.

## VMkernel Module Loader

The program `vmkload_mod` is used to load device driver and network shaper modules into the VMkernel. `vmkload_mod` can also be used to unload a module, list the loaded modules and list the available parameters for each module.

The format for the command is

```
vmkload_mod <options> <module-binary> <module-tag> \
<parameters>
```

**Note:** The command should be typed on one line. Do not type the backslash.

`<module-binary>` is the name of the module binary that is being loaded.

`<module-tag>` is the name that the VMkernel associates with the loaded module. The tag can be any string of letters and numbers. If the module is a device driver, the VMkernel names the module with the `<module-tag>` plus a number starting from zero. If there are multiple device instances created by loading the module or multiple device driver modules loaded with the same tag, each device gets a unique number based on the order in which device instances are created.

The `<module-binary>` and `<module-tag>` parts of the command line are required when a module is loaded and are ignored when the `--unload`, `--list` and `--showparam` options are used. The `<parameters>` part of the command line is optional and is used only when a module is being loaded.

### Options

**-l**

**--list**

List out the current modules loaded. If the **-l** option is given, other arguments on the command line are ignored.

**-u <module-binary>**

**--unload <module-binary>**

Unload the module named **<module-binary>**.

**-v**

**--verbose**

Be verbose during the module loading.

**-d <scsi-device-name>**

**--device <scsi-device-name>**

The module being loaded is for a SCSI adapter that is currently being used by the console operating system. After the module is loaded the SCSI adapter is controlled by the VMkernel but the console operating system continues to be able to access all SCSI devices. The format of **<scsi-device-name>** is

**<PCI-Bus>:<PCI-slot>**.

**-e**

**--exportsym**

Export all global exported symbols from this module. This allows other modules to use exported functions and variables from the loaded module. This option should not be used for normal device driver and shaper modules since there may be symbol conflicts.

**-s**

**--showparam**

List all available module parameters that can be specified in the **<parameter>** section of the command line.

### Parameters

Modules can specify parameters that can be set on the command line. A list of these parameters is shown via the **--showparam** option. In order to set one of these parameters, you must specify a name-value pair at the end of the command line. The syntax is of the form **<name>=<value>**. Any number of parameters can be specified.

### Examples

```
vmkload_mod ~/modules/e100.o vmnic debug=5
```

loads the module `~/modules/e100.o` into the VMkernel. The tag for this module is `vmnic`. Each EEPro card that was assigned to the VMkernel is given the name `vmnic<#>`, where `<#>` starts at 0. For example, if there are two EEPro cards assigned to the VMkernel, they have VMkernel names of `vmnic0` and `vmnic1`. The module parameter `debug` is set to the value 5.

```
vmkload_mod --device 0:12 ~/modules/aic7xxx.o vmhba
```

loads the module `~/modules/aic7xxx.o` into the VMkernel. The tag for this module is `vmhba`. The Adaptec SCSI adapter is currently being used by the console operating system. The SCSI adapter is located on PCI bus 0, slot 12.

```
vmkload_mod --exportsym ~/modules/vmklinux linuxdrivers
```

loads the module `~/modules/vmklinux` into the VMkernel. All exported symbols from this module are available to other modules that are subsequently loaded. The `vmklinux` module is the module that allows Linux device drivers to run in the VMkernel so it is one of the few modules for which the `--exportsym` option makes sense.

Here are several examples of command lines that load various modules:

### Preparing to Load Modules

```
vmkload_mod -e /usr/lib/vmware/vmkmod/vmklinux linux
```

This command must be given before you load other device modules. It loads common code that allows the VMkernel to make use of modules derived from Linux device drivers to manage its high-performance devices. The `-e` option is required so that the `vmklinux` module exports its symbols, making them available for use by other modules.

### Loading Modules

```
vmkload_mod /usr/lib/vmware/vmkmod/e100.o vmnic
```

```
vmkload_mod /usr/lib/vmware/vmkmod/aic7xxx.o vmhba
```

The first of these commands loads a module to control the EEPro Ethernet device(s) reserved for the VMkernel. The second loads a module to control the Adaptec SCSI device(s). The last argument supplied (`vmnic` and `vmhba` in the above examples) determines the base name that VMware uses to refer to the device(s) in the VMware virtual machine configuration file.

For example, suppose your machine has two EEPro Ethernet cards and three Adaptec SCSI cards, and you assigned one Ethernet card and two SCSI cards to the VMkernel during the installation process. After you issue the two commands above, the EEPro



Ethernet card assigned to the VMkernel is given the name `vmnic0` and the two SCSI cards assigned to the VMkernel are given the names `vmhba0` and `vmhba1`.

**Note:** You only need to load the Adaptec VMkernel module once, even though two Adaptec SCSI cards are assigned to the VMkernel.

The VMkernel can also share SCSI adapters with the console operating system, rather than exclusively controlling them. The installation process allows you to specify SCSI adapters that are shared and load the device module appropriately. However, if you wish to control the sharing explicitly, assign the SCSI device to the console operating system during the installation process. Then load the VMkernel SCSI module using the following syntax:

```
vmkload_mod -d bus:slot \  
/usr/lib/vmware/vmkmod/aic7xxx.o vmhba
```

**Note:** This command should be entered on a single line. Do not type the backslash.

To obtain the bus and slot (also known as device or cardnum) information, examine `/proc/pci`, output from the `scanpci` command, or both.

**Note:** The device must be correctly assigned to the console operating system. Devices assigned exclusively to the VMkernel during the installation process no longer appear in `/proc/pci`.

After you load a VMkernel device module, an entry appears in `/proc/vmware/net` or `/proc/vmware/scsi`. For example, when `e100.o` is loaded as described above, the entry `/proc/vmware/net/vmnic0` appears, indicating there is one EEPro card controlled by the VMkernel and available as `vmnic0` to the virtual machines. See [Configuring Virtual Machines on page 181](#) for information on how to configure virtual machines to use VMkernel devices.

### Other Information about VMkernel Modules

The only non-device VMkernel module available in this release of VMware ESX Server is the `nfshaper` module, which provides support for network filtering, as described in [Network Bandwidth Management on page 253](#). Load `nfshaper` using the following syntax.

```
vmkload_mod /usr/lib/vmware/vmkmod/nfshaper.o nfshaper
```

VMkernel modules must be reloaded each time the VMkernel is loaded (as described in [Loading VMkernel Device Modules on page 174](#)). If you have configured your system to load the VMkernel automatically on each reboot, you can have the modules loaded automatically as well by adding entries to the file `/etc/vmware/vmkmoudle.conf`. The `vmkmoudle.conf` file is read only if it

contains a comment line containing the keyword `MANUAL-CONFIG`. Otherwise, the configuration is obtained automatically from the database of the management interface.

Each line that is not blank and does not begin with `#` should contain the name of a module file, the tag to be associated with the module in the VMkernel and possibly a sharing specification (the argument specified with the `-d` flag above). The module file should just be the base file name, without the `/usr/lib/vmware/...` path. A sample `vmkmodule.conf` file is:

```
# MANUAL-CONFIG
vmklinux.o linux
nfshaper.o nfshaper
e100.o vmnic
aic7xxx.o vmhba -d 0:1
```

# 6

## **Configuring and Running Virtual Machines**

# Configuring and Running Virtual Machines

This section contains the following:

- [Configuring Virtual Machines on page 181](#)
  - [Using VMkernel Devices on page 182](#)
  - [Modifying the SMBIOS UUID on page 187](#)
  - [Recommended Configuration Options on page 186](#)
- [Suspending and Resuming Virtual Machines on page 190](#)
  - [Setting the Suspend Directory on page 190](#)
  - [Enabling Repeatable Resumes on page 191](#)
- [Authentication and Security Features on page 193](#)
  - [Authenticating Users on page 193](#)
  - [Default Permissions on page 194](#)

# Configuring Virtual Machines

This section contains the following:

- [Using VMkernel Devices on page 182](#)
  - [Ethernet on page 182](#)
  - [VMFS Virtual SCSI Disks on page 182](#)
  - [Access Modes on page 183](#)
  - [Virtual SCSI Disks on the Console Operating System on page 184](#)
  - [Naming VMFS File Systems on page 185](#)
- [Recommended Configuration Options on page 186](#)
  - [SleepWhenIdle on page 186](#)
- [Modifying the SMBIOS UUID on page 187](#)

The simplest way to set up a new virtual machine is to use the Setup Wizard, as described in [Using the Setup Wizard to Configure Your Server on page 33](#).

Key configuration settings for an existing virtual machine can be changed from the VMware Management Interface. The virtual machine must be powered off when you change the configuration.

1. Log in to the server from the VMware Management Interface (`http://<hostname>/`) as a user who has rights to change the configuration file.
2. From the server's overview page (`http://<hostname>/overview`), click the link under the name of the virtual machine you want to reconfigure.
3. On the details page for that virtual machine, click **Edit VM Configuration**.
4. Make any changes you wish to the configuration, then click **Save Changes**.

To modify other settings in the configuration, manually edit the configuration file as described in this section. You may use the configuration file editor in the VMware Management Interface (point to the terminal icon for the virtual machine, then click **Edit Configuration > Use Text Editor**) or log in to the console operating system and use a text editor there. For purposes of illustration, we assume that you are working with the file `newvm.cfg` in a directory named `/virtual_machines/vml`.

There may also be situations when you want to create virtual machines that are more complex than you can create using the VMware Management Interface. In these cases, start with the configuration file template, `/usr/share/doc/vmware/sample.cfg`. Copy it to a new file and manually edit the copy as described in this section.

### Using VMkernel Devices

The VMkernel devices — whether shared or not — must be referenced and activated in the VMware virtual machine's configuration (`.cfg`) file, as described in this section. You must also load a special VMware network driver into the guest operating system, as described in the section [Installing VMware Tools and the Network Driver in the Guest Operating System on page 73](#).

#### Ethernet

The Ethernet section of the configuration file is in this format:

```
ethernet0.present = TRUE
ethernet0.connectionType = monitor_dev
ethernet0.virtualDev = vmxnet
ethernet0.devName = vmnic0
ethernet0.exclusive = TRUE
```

In this configuration, `ethernet0.connectionType = monitor_dev` and `ethernet0.virtualDev = vmxnet` specify that the virtual machine's Ethernet uses the VMkernel high-performance network device. `ethernet0.devName = vmnic0` specifies that the virtual network device corresponds to the first network device activated by the command `vmkload_mod .../vmkernel .../XXX.o vmnic`. See [VMkernel Module Loader on page 174](#) for details on `vmkload_mod`. The line `ethernet0.exclusive = TRUE` makes the networking more efficient if only one virtual machine is using the network card. You should remove this line if more than one virtual machine needs to use the card.

#### VMFS Virtual SCSI Disks

VMware ESX Server supports a simple file system known as VMFS (VMware ESX Server File System) on physical SCSI disks and partitions to make it easy to allocate space for a disk image. VMFS allows many disk images to be stored on one large physical SCSI disk or partition. The VMware Management Interface automatically creates VMFS file systems and VMFS files as you configure your system and create virtual machines. However, VMFS files can also be created and managed via the `vmkfstools (1)` command. An example configuration that uses a disk image allocated in a VMFS is:

```
scsi0.present = TRUE
scsi0.virtualDev = vmxbuslogic

scsi0:2.present = TRUE
scsi0:2.name = vmhba1:3:0:2:data.dsk
```

In this configuration, `scsi0.present = TRUE` specifies that the virtual machine has a SCSI adapter called `scsi0` and `scsi0.virtualDev = vmxbuslogic` specifies that the virtual machine's first SCSI adapter accesses data from the VMkernel SCSI device. Finally, `scsi0:2.name = vmhba1:3:0:2:data.dsk` specifies the location of the disk image used for SCSI target 2 on the first virtual SCSI adapter.

The location of the disk image is specified in a notation with the form `<adaptername>:<target>:<lun>:<partition>:<filename>`. An adapter name such as `vmhba1` specifies the second physical SCSI adapter activated by the `vmkload_mod .../XXX.o vmhba` command. The second component of the location specifies the ID of the target on the named adapter. The third component specifies the LUN (logical unit number) and is typically zero. The fourth component specifies the partition. The last component specifies the name of the disk image in the VMFS file system on the specified partition.

So `scsi0:2.name=vmhba1:3:0:2:data.dsk` indicates that the disk image is in the file `data.dsk` on partition 2 of the disk at target 3 and LUN 0 on the second SCSI adapter activated by the `vmkload_mod .../XXX.o vmhba` command. See [VMkernel Module Loader on page 174](#) for details on `vmkload_mod`.

A specification may have a partition specified as 0, in which case it refers to a VMFS that covers a complete, unpartitioned disk (target). However, if your SCSI adapter is shared with the console operating system, rather than assigned exclusively to the VMkernel, you cannot access a VMFS that covers the entire disk. Thus, we recommend that you always create at least one partition on each disk and create the VMFS within that partition.

For information on copying an existing virtual disk from the console operating system to a VMFS file, see [Migrating VMware Workstation and VMware GSX Server Virtual Machines on page 71](#).

**Note:** If you have not determined which SCSI target ID corresponds to the disk you wish to use in the virtual machine, see [Determining SCSI Target IDs on page 208](#).

### Access Modes

By default, disk images are accessed in persistent mode. That is, all changes are written directly to the disk image and cannot be undone. This mode provides the most efficient access to the data. ESX Server also supports nonpersistent, undoable and

append modes. You can change the disk mode setting on the Edit VM Configuration page of the VMware Management Interface. The virtual machine must be powered down before you change the disk mode. You can also make the changes directly in the configuration file by including lines in the following format:

```
scsi0:2.mode = nonpersistent
```

or

```
scsi0:2.mode = undoable
```

If the mode of a disk image is nonpersistent, any changes to the disk are lost when the associated virtual machine shuts down. If the mode of the disk image is undoable, the changes are maintained in a separate file, known as the redo log, on the SCSI disk. Each time the virtual machine is powered down, a dialog asks whether changes made to the disk during the current session should be discarded, committed to the base disk image or appended (kept in the redo log).

VMware ESX Server supports an additional append mode for disk images stored as VMFS files. Like undoable mode, append mode maintains a redo log. However, in this mode, no dialog appears when the virtual machine is powered off to ask whether you want to commit changes. All changes are continually appended to the redo log. At any point, you can undo all the changes by removing the redo log. Its name is derived from the original name of the file that contains the disk by adding `.REDO`. Changes can be committed permanently to the base disk image via the commit option of the `vmkfstools` command. For details on this command, see [Using vmkfstools on page 199](#).

### Virtual SCSI Disks on the Console Operating System

VMware ESX Server also supports virtual SCSI disks that are stored on the file system of the console operating system. Virtual SCSI disks created under VMware Workstation 2.0 and higher are supported, although a new network driver needs to be loaded into the guest operating system. Disks created under VMware GSX Server are also supported. For details, see [Migrating VMware Workstation and VMware GSX Server Virtual Machines on page 71](#).

To create a new, blank virtual SCSI disk for your virtual machine, copy the file `/usr/lib/vmware/virt-scsi.dsk` from the ESX Server installation CD-ROM to the working directory for your virtual machine.

```
cp virt-scsi.dsk /virtual_machines/vml/virt-scsi.dsk
```

Then add lines to your virtual machine's configuration file to describe the new disk. Those lines have the following format:



```
scsi0.present = TRUE
scsi0.virtualDev = buslogic

scsi0:1.present = TRUE
scsi0:1.fileName = virt-scsi.dsk
scsi0:1.mode = nonpersistent
```

**Note:** Using virtual disks stored on the console operating system's file system does not take advantage of ESX Server's new high-performance SCSI disk architecture and therefore the performance of the virtual machine may suffer.

### Naming VMFS File Systems

If you create a VMFS file system on a SCSI disk or partition, you can give a name to that file system and use that name when specifying VMFS files on that file system. For instance, suppose you have a VMFS file system on the SCSI partition `vmhba0:3:1` and have created a VMFS file `nt4.dsk`. You can name that file system either using the Web-based configuration wizard or via a `vmkfstools` command such as

```
vmkfstools -S mydisk vmhba0:3:1:0
```

You can then refer to the `nt4.dsk` file as `mydisk:nt4.dsk` (instead of `vmhba0:3:1:0:nt4.dsk`) in a virtual machine configuration file and in other `vmkfstools` commands.

Naming VMFS file systems is especially useful if you may be adding SCSI adapters or disks to your system. In that case, the actual disk and target numbers specifying a particular VMFS may change, but the name stays the same.

### Recommended Configuration Options

This section details options that can influence the performance of your virtual machines. These settings are not required to run VMware ESX Server correctly.

#### SleepWhenIdle

The configuration file option `monitor.SleepWhenIdle` determines whether the VMkernel deschedules an idle virtual machine. By default, this option is enabled, a setting that ensures much better performance when running multiple virtual machines.

When you are running only a single virtual machine (such as for benchmarking VMware ESX Server), add the following line to the virtual machine's configuration (`.cfg`) file if you want to achieve the best possible performance in the virtual machine (at the expense of responsiveness in the console operating system):

```
monitor.SleepWhenIdle = 0
```

### Modifying the SMBIOS UUID

Each ESX Server virtual machine is automatically assigned a universally unique identifier (UUID), which is stored in the SMBIOS system information descriptor. It can be accessed by standard SMBIOS scanning software — for example SiSoftware Sandra or the IBM utility `smbios2` — and used for systems management in the same ways you use the UUID of a physical computer.

The UUID is a 128-bit integer. The 16 bytes of this value are separated by spaces except for a dash between the eighth and ninth hexadecimal pairs. So a sample UUID might look like this:

```
00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff
```

### Generating the UUID Automatically

The automatically generated UUID is based on the physical computer's identifier and the path to the virtual machine's configuration file. This UUID is generated when you power on or reset the virtual machine. The UUID that is generated remains the same so long as the virtual machine is not moved or copied.

The automatically generated UUID is also written to the virtual machine's configuration file as the value of `uuid.location`.

If you move or copy the virtual machine, a new UUID is generated when the virtual machine is powered on — based on the physical computer's identifier and path to the virtual machine's configuration file in its new location.

If you suspend and resume a virtual machine, this does not trigger the process that generates a UUID. Thus, the UUID in use at the time the virtual machine was suspended remains in use when the virtual machine is resumed, even if it has been copied or moved. However, the next time the virtual machine is rebooted, the UUID is generated again. If the virtual machine has been copied or moved, the UUID is changed.

In some circumstances — for example, if you are moving the virtual machine but want to keep the same UUID — you may want to assign a specific UUID to the virtual machine. In that case, you need to override the automatically generated UUID value. To do so, edit the virtual machine's configuration file as described in this section to set the value of the parameter `uuid.bios`.

### Comparing the Generated UUID to Configuration File Parameters

When a virtual machine is powered on, ESX Server generates a UUID as described above and compares it to the values for `uuid.location` and (if it exists) `uuid.bios` in the configuration file.

If the automatically generated UUID matches the value of `uuid.location`, ESX Server checks for `uuid.bios`. If `uuid.bios` exists, its value is used as the virtual machine's UUID. If `uuid.bios` does not exist, the automatically generated value is used.

If the automatically generated UUID does not match the value of `uuid.location`, the newly generated value is used as the virtual machine's UUID and is saved to the configuration file, replacing the previous value of `uuid.location` and (if it exists) `uuid.bios`.

**Note:** Any changes to the UUID take effect only after the virtual machine is rebooted.

### Setting the UUID for a Virtual Machine that Is Not Being Moved

To assign a specific UUID to a virtual machine that is not being moved, add one line to the configuration file. You may use the configuration file editor in the VMware Management Interface (point to the terminal icon for the virtual machine, then click **Edit Configuration > Use Text Editor**) or log in to the console operating system and use a text editor there. The format for the line is:

```
uuid.bios = <uuidvalue>
```

The UUID value must be surrounded by quotation marks. A sample configuration line might look like this:

```
uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"
```

After adding this line to the configuration file, restart the virtual machine. The new UUID is used when the virtual machine restarts.

### Setting the UUID for a Virtual Machine that Is Being Moved

If you plan to move a virtual machine and want it to have the same UUID it did before the move, you must note the UUID being used before the move and add that UUID to the configuration file after the move. Follow these steps:

1. Before moving the virtual machine, examine its configuration file. You may use the configuration file editor in the VMware Management Interface (point to the terminal icon for the virtual machine, then click **Edit Configuration > Use Text Editor**) or log in to the console operating system and use a text editor there.

If the virtual machine's UUID has been set to a specific value, the configuration file has a line that begins with `uuid.bios`. Note the 128-bit hexadecimal value that follows. This is the value you should use in the new location.

If there is no line beginning with `uuid.bios`, look for the line that begins with `uuid.location` and note the 128-bit hexadecimal value that follows it.

2. Move the virtual machine's disk (`.disk`) file to the new location.

3. Use the VMware Management Interface to create a new virtual machine configuration and set it to use the virtual disk file you moved in the previous step.
4. Start the virtual machine, then shut it down.
5. Edit the virtual machine's configuration file to add a `uuid.bios` line, as described in [Setting the UUID for a Virtual Machine that Is Not Being Moved on page 188](#). Set the value of `uuid.bios` to the value you recorded in step 1.
6. Start the virtual machine. It should now have the same UUID as it did before the move.

# Suspending and Resuming Virtual Machines

This section contains the following:

- [Setting the Suspend Directory on page 190](#)
- [Enabling Repeatable Resumes on page 191](#)

Suspending a virtual machine, then later resuming its operation, can speed provisioning tasks — for example, deployment of standby servers. VMware ESX Server supports two configurations for resuming a suspended virtual machine.

- You can suspend a running virtual machine at any time, then resume operation, suspend at a later time, then resume with the machine in the second state, and so on.
- You can suspend a virtual machine at any desired point in its operation, then lock in the suspended state at that chosen point. Any time you restart the virtual machine, it resumes in the same state — the state it was in when you first suspended it.

**Note:** You should not change a configuration file after you suspend a virtual machine, since the virtual machine does not resume properly if the configuration file is inconsistent with the suspended virtual machine. Also, you should not move any physical disks or change the name of any VMFS file systems that the virtual machine uses. If you do, the virtual machine will not be able to access its virtual disks when it resumes.

You can also set the configuration of each virtual machine so the file that stores information on the suspended state is saved in a location of your choice.

**Note:** You cannot suspend a virtual machine configured to use more than 2GB of RAM.

## Setting the Suspend Directory

When a virtual machine is suspended, its state is written to a file with a `.vmss` extension. By default, the `.vmss` file is written to the same directory as the configuration file. Similarly, when a virtual machine is being resumed, ESX Server looks for the `.vmss` file in the same directory as the configuration file.

You may want to select a different location for better performance or to avoid running out of space on the partition that holds the virtual machine directories.

When you change the directory where the suspended state file for a virtual machine is stored, the virtual machine must be powered off. Then follow these steps:

1. Log in to the VMware Management Interface, point to the terminal icon for the virtual machine you want to change, then click **Edit Configuration**. Scroll to the bottom of the page to the Misc. section and select the desired suspend location.

For fastest suspend and restore operations, select **VMFS Volume** and choose the appropriate VMFS volume from the drop-down list. ESX Server automatically adds a suffix to the name of the suspended state file to ensure that one virtual machine does not overwrite the suspended state file of another.

If you want to save the suspend file in a different directory, specify the path in the **Other location** entry field.

2. Click **Save Changes**.

### Enabling Repeatable Resumes

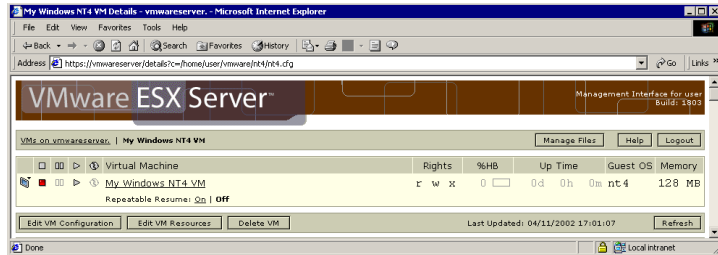
When you suspend a virtual machine in the usual way, by clicking the suspend button on the remote console or in the management interface, ESX Server writes a file with a `.vmss` extension. This file contains the entire state of the virtual machine. When the virtual machine is resumed, its state is restored from the `.vmss` file. The `.vmss` file is then modified while the virtual machine is running. This means that, in normal operation, the `.vmss` file cannot be used to resume a virtual machine again from the original suspended state.

If you do want to be able to resume a virtual machine in the same state repeatedly — for example, to have a hot-standby virtual machine in a particular state so it is ready to take over for a failed server — take the following steps:

1. Shut down and power off the virtual machine.
2. Be sure all virtual disks used by the virtual machine are set to nonpersistent mode.

On the main page of the VMware Management Interface, move the mouse pointer above the terminal icon for the virtual machine you want to set for repeatable resume mode. A context menu appears. Choose **Edit Configuration** to go to the Configure VM page, where you can set the disk mode. You have access to this page only when the virtual machine is powered off.

After making your changes, click **Save Changes**. ESX Server saves your changes and takes you to the details page for the virtual machine.



3. Next to Repeatable Resume, click **On** to enable the repeatable resume feature.
4. Power on the virtual machine.
5. Using the remote console, take the steps necessary to reach the state in which you want to suspend the virtual machine.
6. Click **Suspend** to activate repeatable resume.
7. After you do this, each time you resume the virtual machine, it will resume from the suspend point you have set. When you click **Power Off**, the virtual machine will power off, ready to resume at the suspend point you have set.

To turn off the repeatable resume feature, take the following steps while the virtual machine is running.

1. On the main page of the VMWare Management Interface, click the name of the virtual machine you want to take out of repeatable resume mode.
2. On the details page for the virtual machine, next to Repeatable Resume, click Off to disable and deactivate the repeatable resume feature.



## Authentication and Security Features

This section contains the following:

- [Authenticating Users on page 193](#)
- [Default Permissions on page 194](#)
- [TCP/IP Ports for Management Access on page 194](#)

There are three key aspects to security with VMware ESX Server.

- VMware ESX Server authenticates all remote users who connect to a server using the VMware Management Interface or the remote console.
- Security for network traffic to and from the server depends on the security settings in the server configuration.
- Three or more TCP/IP ports are used for access, depending on the security settings in your ESX Server configuration.

Depending on your remote access requirements, you may need to configure your firewall to allow access on one or more of these ports. For details on which ports are used, see [TCP/IP Ports for Management Access on page 194](#).

### Authenticating Users

VMware ESX Server uses Pluggable Authentication Modules (PAM) for user authentication in the remote console and the VMware Management Interface. The default installation of ESX Server uses `/etc/passwd` authentication, just as Linux does, but it can easily be configured to use LDAP, NIS, Kerberos or another distributed authentication mechanism.

The PAM configuration is in `/etc/pam.d/vmware-authd`.

Every time a connection is made to the server running VMware ESX Server, the `inetd` process runs an instance of the VMware authentication daemon (`vmware-authd`). The `vmware-authd` process requests a user name and password, then hands them off to PAM, which performs the authentication.

Once a user is authenticated, `vmware-authd` accepts a path name to a virtual machine configuration file. Access to the configuration file is restricted in the following ways:

- The user must have **read** access to the configuration file to see and control the virtual machine in the VMware Management Interface and to view the Details and Event Log pages.

- The user must have **read** access to the configuration file to use the local console on the console operating system or to connect to the virtual machine with the VMware Perl API.
- The user must have **read** and **execute** access to the configuration file to connect to and control (start, stop, reset or suspend) a virtual machine in a remote console, with the VMware Perl API or with the management interface.
- The user must have **read** and **write** access to the configuration file to change the configuration using the Configure VM page in the VMware Management Interface.

**Note:** If you have users with **list** access, but not **read** access, they may encounter errors in the VMware Management Interface.

If a `vmware` process is not running for the configuration file you are trying to use, `vmware-authd` examines `/etc/vmware/vm-list`, the file where you register your virtual machines. If the configuration file is listed in `vm-list`, `vmware-authd` (not necessarily the user who is currently authenticated) starts VMware ESX Server as owner of this configuration file.

Registered virtual machines (those listed in `/etc/vmware/vm-list`) also appear in the VMware Management Interface. The virtual machines you see on the Overview page must be listed in `vm-list`, and you must have read access to their configuration files.

The `vmware-authd` process exits as soon as a connection to a `vmware` process is established. Each `vmware` process shuts down automatically after the last user disconnects.

### Default Permissions

When you create a virtual machine with VMware ESX Server, its configuration file is registered with the following default permissions, based on the user accessing it:

- Read, execute and write — for the user who created the configuration file (the owner)
- Read and execute — for the owner's group
- Read — for users other than the owner or a member of the owner's group

### TCP/IP Ports for Management Access

The TCP/IP ports available for management access to your ESX Server machine vary, depending on the security settings you choose for the server. If you need to manage ESX Server machines from outside a firewall, you may need to reconfigure the firewall

to allow access on the appropriate ports. The lists below show which ports are available when you use each of the standard security settings.

The key ports for use of the VMware Management Interface and the remote console are the HTTP or HTTPS port and the port used by `vmware-authd`. Use of other ports is optional.

### High Security

- 443 – HTTPS, used by the VMware Management Interface
- 902 – `vmware-authd`, used when you connect with the remote console
- 22 – SSH, used for a secure shell connection to the console operating system

### Medium Security

- 443 – HTTPS, used by the VMware Management Interface
- 902 – `vmware-authd`, used when you connect with the remote console
- 22 – SSH, used for a secure shell connection to the console operating system
- 23 – Telnet, used for an insecure shell connection to the console operating system
- 21 – FTP, used for transferring files to and from other machines
- 111 – `portmap`, used by the NFS client when mounting a drive on a remote machine

### Low Security

- 80 – HTTP, used by the VMware Management Interface
- 902 – `vmware-authd`, used when you connect with the remote console
- 22 – SSH, used for a secure shell connection to the console operating system
- 23 – Telnet, used for an insecure shell connection to the console operating system
- 21 – FTP, used for transferring files to and from other machines
- 111 – `portmap`, used by the NFS client when mounting a drive on a remote machine



7

## **Disks**

## Disks

This section provides the following information:

- [File System Management on SCSI Disks and RAID on page 199](#)
  - [Using vmkfstools on page 199](#)
  - [Naming VMFS File Systems on page 205](#)
  - [Mounting VMFS File Systems on the Console Operating System on page 205](#)
- [Utility to Mount VMFS File Systems on page 206](#)
- [Determining SCSI Target IDs on page 208](#)
- [Sharing the SCSI Bus on page 210](#)
- [Using Storage Area Networks with ESX Server on page 212](#)

## File System Management on SCSI Disks and RAID

The VMFS file system is a simple, high-performance file system on physical SCSI disks and partitions, used for storing large files such as the disk images for ESX Server virtual machines and, optionally, the memory images of suspended virtual machines. A server's VMFS file systems are mounted automatically by the console operating system and appear in the `/vmfs` directory.

Files in these mounted VMFS file systems can be viewed and manipulated with ordinary file commands such as `ls` and `cp`. As noted later in this section, there are limitations when you use some standard disk utilities with files in a VMFS file system — limitations caused by the fact that the utilities often assume a file is no larger than 2GB. The `vmkfstools` program provides additional functions that are particularly useful when you need to create files of a particular size and when you need to import files from and export files to the console operating system's file system. In addition, `vmkfstools` is designed to work with large files, overcoming the 2GB limit of some standard file utilities.

### Using vmkfstools

To create and manipulate files on SCSI disks managed by VMware ESX Server, use `vmkfstools`. It supports the creation of a VMware ESX Server file system (VMFS) on a SCSI disk or partition and the management of files stored in the VMFS. It is useful for storing multiple virtual disk images on a single SCSI disk or partition of a SCSI disk.

The format for the command is

```
vmkfstools <options> <device>[:<file>]
```

The `vmkfstools` command is issued with a device specification and one or more options.

`<device>` specifies a SCSI device (a SCSI disk or a partition on a SCSI disk) being manipulated and `<options>` specifies the operation to be performed.

`<device>` is specified in a form such as:

```
vmhba1:2:0:3
```

Here, `vmhba1` specifies the second SCSI adapter activated by the command `vmkload_mod .../XXX.o vmhba`. (See [VMkernel Module Loader on page 174](#) for details on `vmkload_mod`.) The second number specifies the target on the adapter, the third number specifies the LUN (logical unit number) and the fourth

number specifies the partition. If the partition number is zero, the whole disk is implied; otherwise, the indicated partition is specified.

<device> may also be a VMFS file system name, as set in the management interface or with the `vmkfstools --setfsname` command.

<file> is the name of a file stored in the file system on the specified device.

### Options

The long and short forms of options, shown together in this list, are equivalent.

`-C --createfs`

`-b --blocksize # [mMkK]`

`-n --numfiles #`

Create a VMFS file system on the specified SCSI device. The file block size can be specified via the `-b` option. The block size must be at least 1MB and must be a power of 2. The maximum number of files in the file system can be specified with the `-n` option. The default maximum is 256 files.

`-N --consolename`

Print out the name of a Linux device that represents the specified SCSI device on the console operating system. The resulting device name can be used in accessing the SCSI device via commands such as `fdisk` on the console operating system. The association between the Linux device name and the specified SCSI device lasts only until ESX Server is unloaded or the machine is rebooted.

`-F --config [private|public|shared|writable]`

Set the VMFS file system on the specified SCSI device to the specified mode.

The default mode of a VMFS file system is private, which means the VMFS is accessed by only a single ESX Server computer.

A VMFS file system that may be accessed by multiple ESX Server computers (for example, a VMFS on a disk on a storage area network) should have its mode set to public. VMFS file systems set to public mode will have automatic locking to ensure that they are not accessed by more than one ESX Server computer simultaneously.

A VMFS file system that will be used for failover-based clustering should have its mode set to shared. This mode allows virtual machines on multiple servers to access the same VMFS file simultaneously. However, when the virtual machines access a file on a shared VMFS, the file system metadata will become read-only. That is, no virtual machine or user command will be allowed to create, delete or change the attributes of a file. When virtual machines are no longer accessing the VMFS file system, the file system metadata can be made writable again with the command `vmkfstools --config writable`.



**-R --recover**

Recover a VMFS file system (that is accessible by multiple ESX servers) when other vmfstools commands indicate that the file system is locked by another ESX server, but no other server is currently accessing. This situation may happen if the VMFS file system was being accessed by a server (e.g. running a virtual machine or mounting the VMFS via mount-vmfs) and that server crashed. You should only use this command if you are certain that no other server is still accessing the file system.

**-c --createfile #[mMkK]**

Create a file with the specified size on the file system of the specified SCSI device. The size is specified in bytes by default, but it can be specified in kilobytes or megabytes by adding a suffix of **k** or **m** respectively.

**-a --accessperm <uid> <gid> <mode>**

Set the access permissions of the specified VMFS file. The user ID and group ID of the file are set to **<uid>** and **<gid>**, respectively, and the access permissions of the file are set to **<mode>**. The permission bits are specified in octal, and are as specified in the **chmod (2)** man page.

**-e --exportfile <dstFile>**

Export the contents of the specified file on the specified SCSI device to a virtual disk on the file system of the console operating system. The virtual disk may then be transferred to another machine and imported to a SCSI device on the remote machine. Hence the combination of **exportfile** and **importfile** may be used for copying VMFS files to remote machines. The virtual disk likely takes less space than the full size of the VMFS file, since the virtual disk does not include zeroed sectors of the VMFS file.

**-d --copyfile <srcFile> or**

**-i --importfile <srcFile>**

Import the contents of a VMware virtual, plain or raw disk on the console operating system to the specified file on the specified SCSI device. This command is often used to import the contents of a VMware Workstation virtual disk onto a SCSI device. It may also be used to import a virtual disk that was created by exporting the contents of a disk from another SCSI device. The complete contents of the source disk are copied, even if it is mostly free space, so the destination device must have space for the entire size of the virtual disk.

**-E --exportraw <dstFile>**

Export the contents of the specified file on the specified SCSI device in unmodified form to a file on the file system of the console operating system. This command differs from **exportfile** in that it copies the source file exactly, rather than creating a

virtual disk. Since the console operating system has a maximum file size of 2GB, this command is not useful for large disk images; use `exportfile` instead. However, `exportraw` is useful for distributing incremental updates to a disk image. If the disk image is used in undoable or append mode, then a redo log file is created. The name of that file is derived by appending `.REDO` to the name of the associated disk image file. The redo log contains the incremental changes to the disk image. The contents of the redo log can be copied to the file system of the console operating system using the `exportraw` command. The redo log can then be transported to a remote site and copied to the SCSI disk that contains a copy of the original disk image with the `importraw` command. The contents of the redo log can then be merged into the copy of the disk image using the `commit` command.

`-I --importraw <srcFile>`

Import the exact contents of the specified file on the console operating system to the specified file on the specified SCSI device. This command differs from `importfile` in that it copies the source file exactly. As explained in the discussion of `exportraw` above, the combination of `exportraw` and `importraw` is useful for distributing incremental updates to a disk image.

`-l --list`

List the files on the file system on the specified device, including their permissions, sizes and last-modified times.

`-r --removefile`

Remove the specified file from the file system on the specified device.

`-r --renamefile <newName>`

Rename the specified VMFS file to the specified new name.

`-m --commit`

Commit the redo log of the specified file, making the associated changes permanent. The redo log is created when a file is used in undoable mode or append mode via a virtual machine. The name of the redo log is derived by appending `.REDO` to the name of the file that contains the base disk image. The changes to the disk that are stored in the redo log can either be committed using the `commit` option or be eliminated by removing the redo-log file using the `remove` option.

`-w --createswapfile # [mMkK]`

Create a swap file with the specified size on the VMFS file system of the specified SCSI device. The size is specified in bytes by default, but can be specified in kilobytes or megabytes by adding a suffix of `k` or `m` respectively. ESX Server immediately starts using the swap file after it is created. This command is also used to activate an existing

swap file. If the specified length is different from the length of the existing swap file, the length of the swap file is changed.

**-S --setfsname <fsName>**

Set the name of the VMFS file system on the specified SCSI device to **<fsName>**. This name can then be used to specify a VMFS file in subsequent **vmkfstools** commands or in a virtual machine configuration file. The name also appears in a listing produced by **vmkfstools -l**.

**-X --extendfile #[mMkK]**

Extend the specified VMFS file to the specified length. Use this command to extend the size of a disk allocated to a virtual machine after the virtual machine has been created. The virtual machine that uses this disk file must be powered off when you enter this command. The guest operating system must be able to recognize and use the new size of the disk, for example by updating the file system on the disk to take advantage of the extra space.

### Examples

```
vmkfstools -C -b 2m -n 32 vmhba1:3:0:1
```

Create a new file system on the first partition of target 3, LUN 0 of SCSI adapter 1. The file block size is 2MB and the maximum number of files is 32.

```
vmkfstools -S mydisk vmhba1:3:0:1
```

Give the name of **mydisk** to the new file system.

```
vmkfstools -c 2000m mydisk:rh6.2.dsk
```

Create a 2GB VMFS file with the name of **rh6.2.dsk** on the VMFS file system named **mydisk**. This file represents an empty disk and may be accessed by a virtual machine.

```
vmkfstools -r vmhba0:2:0:1:file2
```

Remove the file named **file2** in the file system on target 2, partition 1 of SCSI adapter 0.

```
vmkfstools -i ~/virtual_machines/nt4.dsk
```

```
vmhba0:2:0:0:nt4.dsk
```

Copy the contents of a virtual disk (which contains Windows NT 4.0) from the console operating system's file system to a file named **nt4.dsk** on target 2 of SCSI adapter 0. A virtual machine can be configured to use this virtual disk by adding lines to its configuration file in the following format:

```
scsi0.virtualDev = vmxbuslogic
scsi0:0.present = TRUE
scsi0:0.name = vmhba0:2:0:0:nt4.dsk
```

## Disks

```
vmkfstools -l vmhba0:2:0:0
```

List the contents of the file system on target 2 of SCSI adapter 0.

```
vmkfstools -X 8000M vms:win2000.dsk
```

Expand the virtual disk file named `win2000.dsk` that is stored on a VMFS partition named `vms` to a size of 8GB. The virtual machine that uses this disk file must be powered off before you enter this command. After expanding the disk file, you must run a partition manipulation tool such as PartitionMagic, Volume Manager or ServerMagic in the virtual machine to expand the partition seen by the virtual machine into the newly created space on the virtual disk.

## Naming VMFS File Systems

If you create a VMFS file system on a SCSI disk or partition, you can give a name to that file system and use that name when specifying VMFS files on that file system. For instance, suppose you have a VMFS file system on the SCSI partition `vmhba0:3:0:1` and have created a VMFS file `nt4.dsk`. You can name that file system via a `vmkfstools` commands such as:

```
vmkfstools -S mydisk vmhba0:3:0:1
```

You can then refer to the `nt4.dsk` file as `mydisk:nt4.dsk` (instead of `vmhba0:3:0:1:nt4.dsk`) in a virtual machine configuration file and in other `vmkfstools` commands. Naming VMFS file systems is especially useful if you may be adding SCSI adapters or disks to your system, in which case the actual disk and target numbers specifying a particular VMFS may change, but the name stays the same.

## Mounting VMFS File Systems on the Console Operating System

VMFS file systems are automatically mounted in the `/vmfs` directory on the console operating system when the VMkernel is loaded as the computer boots. The `mount-vmfs` script may be used manually to mount new VMFS file systems. The reverse operation (unmounting all VMFS partitions) can be performed by executing `umount-vmfs`.

Although mounted VMFS file systems may appear similar to any other file system such as ext2, VMFS is only intended to store large files such as disk images. Unfortunately, the console operating system (which is based on a Linux 2.4 kernel) does not currently support files greater than 2GB. NFS and `scp` are known to run into this limitation, while FTP and `cp` are not affected by it. Thus, you should use FTP and `cp` for copying files to and from a VMFS file system.

For more information, see [Utility to Mount VMFS File Systems on page 206](#).

## Utility to Mount VMFS File Systems

`mount-vmfs` is a program that mounts VMFS (VMware ESX Server File System) file systems. It is useful for automatically mounting partitions with valid VMFS file systems on the console operating system.

In its simplest usage, `mount-vmfs` does not take any arguments. It checks every SCSI device available to virtual machines for valid file systems. If a valid file system is found, `mount-vmfs` mounts it at `/vmfs/vmhba<a>:<t>:<l>:<p>`, where `<a>` specifies the SCSI adapter number, `<t>` specifies the SCSI target, `<l>` specifies the LUN (logical unit number) and `<p>` specifies the disk partition. If the disk has no partitions and the disk has a valid file system, `<p>` is zero.

If a partition has an associated file system name (`vmkfstools -S`), then `mount-vmfs` also creates a symbolic link from `/vmfs/<fsname>` to the corresponding mount point (`/vmfs/vmhba<a>:<t>:<l>:<p>`).

The reverse operation — unmounting all VMFS partitions — can be performed by executing `umount-vmfs`.

By default, `mount-vmfs` does not mount any VMFS file systems that have the shared or public attribute. File systems with these attributes set are intended to be accessed by multiple ESX Server computers. Thus, it does not make sense to mount these file systems automatically on any one server. However, `mount-vmfs` will also mount any such file systems if you include the `-F` flag on the command line.

In addition, an individual file system can be mounted explicitly by supplying its device name or file system name as an argument to `mount-vmfs`. The format for the command is

```
mount-vmfs vmhba0:2:0:1
```

This mounts the file system on the specified partition if that partition holds a VMFS file system.

You can use the regular `mount` command to mount VMFS file systems. The file system type is `vmfs` and the device name is `vmhba<a>:<t>:<l>:<p>`. The format for the command is

```
mount -t vmfs vmhba0:1:0:2 /vmfs/vmhba0:1:0:2
```

This mounts partition 2 of the disk with target 1 on the adapter `vmhba0`.

Although VMFS file systems may appear similar to any other file system such as `ext2`, VMFS is mainly intended to store large files such as disk images. It does not support directory hierarchies. New file systems can be created using `vmkfstools -C`.

The reported file length of all VMFS files (disk images) is 512 bytes longer than the disk image. The additional 512 bytes contain certain file attributes such as the size of the disk image represented by the file. VMFS files that are not disk images do not incur this 512-byte overhead.

### Limitations

Disk images tend to be large. Unfortunately, the console operating system does not support files greater than 4GB and there is only limited functionality for files between 2GB and 4GB. The file size field of the `stat` system call has only 32 bits, therefore `stat` returns incorrect information for files equal to or bigger than 4GB. For such files, VMFS returns 4GB-1 as the file size in the `stat` system call. NFS and `scp` are known to run into this limitation, while FTP and `cp` are not affected by it.

VMFS files support standard permissions of read, write and execute for owner, group and other. The files do not support `setuid` or `setgid` flags. The VMFS directory has the same permissions as `/tmp`, which means that anyone can create a file in the directory, but users can read or modify only those files for which they have appropriate permissions.

Currently, VMFS file names are limited to 128 bytes.

For further information, see [File System Management on SCSI Disks and RAID on page 199](#).

## Determining SCSI Target IDs

In order to assign SCSI drives to a virtual machine, you need to know which controller the drive is on and what the SCSI target ID of the controller is. This section can help you determine these values without opening your computer and physically looking at the SCSI target ID settings on the drives.

On a standard Linux system, or for a VMware Console Operating System that has SCSI controllers assigned to the console operating system rather than the VMkernel, information on attached SCSI devices, including SCSI target IDs is available in the boot log (usually `/var/log/messages`), or from examining `/proc/scsi/scsi`.

Information about the SCSI controllers assigned to the VMkernel and about the devices attached to these controllers is available in the `/proc/vmware/scsi` directory once the VMkernel and the VMkernel device module(s) for the SCSI controller(s) have been loaded.

Each entry in the `/proc/vmware/scsi` directory corresponds to a SCSI controller assigned to the VMkernel. For example, assume you issued a `vmkload_mod` command with the base name `vmhba` and a single SCSI controller was found. To identify the controller, type this command:

```
ls -l /proc/vmware/scsi
```

The output of the `ls` command is:

```
total 0
dr-xr-xr-x 2 root  root      0 Jun 22 12:44 vmhba0
```

Each SCSI controller's subdirectory contains entries for the SCSI devices on that controller, numbered by SCSI target ID and LUN (logical unit number). Run `cat` on each target ID:LUN pair to get information about the device with that target ID and LUN. For example, type this command:

```
cat /proc/vmware/scsi/vmhba0/1:0
```

The following information is displayed:

```
Vendor: SEAGATE Model: ST39103LW  Rev: 0002
Type: Direct-Access  ANSI SCSI revision: 02
Size: 8683 Mbytes
Queue Depth: 28
```

```
Partition Info:
Block size: 512
Num Blocks: 17783240
```



## Disks

```
num: Start      Size Type
4:   1  17526914 fb
```

### Partition 0:

```
VM      11
Commands  2
Kbytes read  0
Kbytes written 0
Commands aborted 0
Bus resets  0
```

### Partition 4:

```
Commands  336
Kbytes read 857
Kbytes written 488
Commands aborted 0
Bus resets  0
```

This information should help you determine the SCSI target ID to use in the virtual machine configuration file, as detailed in [Configuring Virtual Machines on page 181](#).

## Sharing the SCSI Bus

Normally, VMware ESX Server enforces locking and does not allow two virtual machines to access the same virtual disk (VMFS file) at the same time. If a second virtual machine tries to access a VMFS file, it gets an error and does not power on.

However, it is often useful to have more than one virtual machine share a disk in order to provide high availability. This configuration is commonly used for disk-based failover, in which one machine takes over running an application when the primary machine fails. The data required for the application is typically stored on a shared disk, so the backup machine can immediately access the necessary data when the failover occurs.

The bus sharing setting is used to determine if virtual machines are allowed to access the same virtual disk simultaneously.

### Setting Bus Sharing Options

Use the VMware Management Interface to change the bus sharing settings for each virtual machine that will access the same virtual disk simultaneously. Log in to the management interface as the appropriate user and be sure the virtual machine you want to configure is powered off. Point to the terminal icon for the virtual machine you want to configure and click **Edit Configuration**. In the SCSI Devices section, choose the bus sharing setting you want, then click **Save Changes**. There are three options.

- **None:** Disks cannot be shared by other virtual machines
- **Virtual:** Disks can be shared by virtual machines on same server
- **Physical:** Disks can be shared by virtual machines on any server

To enable sharing of virtual disks, choose **Virtual** or **Physical**. All virtual disks on the specified virtual bus will be sharable and have the specified mode.

If the bus sharing is virtual, only virtual machines on the same physical machine will be able to share disks. This setting allows for a “cluster-in-a-box” configuration, in which all members of a high-availability cluster are on the same physical machine. This setup is useful for providing high availability when the likely failures are due to software or administrative errors.

If the bus sharing is physical, virtual machines on different physical machines will be able to share disks. In this case, the VMFS holding the virtual disks must be on a physically shared disk, so all of the physical machines can access it. This setup is useful for providing high availability when the likely failures also include hardware errors.

When a shared disk is used for high availability purposes, the current machine that is running the application and using the shared data often reserves the disk using a SCSI command.

If the bus sharing is physical, commands that reserve, reset or release a shared virtual disk are transmitted through to the physical disk, so other machines sharing the disk can properly detect when a virtual disk has been reserved or reset. Therefore, when you are sharing disks among virtual machines across physical machines for high availability purposes, it is often best to put only a single VMFS with a single virtual disk on each shared disk — that is, have only one virtual disk per physical disk. In such a configuration, each virtual disk can be reserved and released independently.

## Using Storage Area Networks with ESX Server

VMware ESX Server can be used effectively with storage area networks (SANs). ESX Server supports Qlogic and Emulex host bus adapters, which allow an ESX Server computer to be connected to a SAN and to see the disk arrays on the SAN.

### Detecting All LUNs

In order to use all storage devices on your SAN, you may need to change some VMkernel configuration options as described below. To make these changes, log in to the VMware Management Interface as root, then go to **Configure System > VMkernel Configuration**. To change an option, click the current value, then enter the new value in the dialog box and click **Update**.

By default, the VMkernel scans for only LUN 0 to LUN 7 for every target. If you are using LUN numbers larger than 7 you must change the setting for DiskMaxLUN field from the default of 8 to the value that you need. For example, if you now have LUN numbers 0 to 15 active, set this option to 16.

By default, the VMkernel is not configured to support sparse LUNs — that is, a case where some LUNs in the range 0 to N are not present, but LUN N is present. If you need to use such a configuration, set the DiskSupportSparseLUN field to 1. (The default is 0.)

### Special Options for SAN Configurations

Because the disks on the SANs can potentially be accessed by multiple ESX Server computers, there are some configuration issues that are unique to SANs.

**Note:** Be sure that only one computer has access to the SAN while you are configuring it for use with ESX Server and formatting it. If the other computers that will access the SAN are also ESX Server machines, they should be powered off while you are configuring the SAN. After you have finished the configuration and checked to be sure all partitions on the shared disk are set for public or shared access (as described in the VMFS Accessibility section below), you may connect and power on the other computers that need access to the SAN.

### VMFS Accessibility

Any VMFS partition on a disk that is on a SAN should have VMFS accessibility set to public or shared, rather than private. Choosing public makes the VMFS partition available to multiple physical servers and to virtual machines on those servers, but

only to a single server at a time. Choose shared to make the VMFS partition available to virtual machines on multiple physical servers at the same time. The shared option is useful for failover-based clustering among virtual machines on multiple servers.

To change the accessibility setting, log in to the management interface as root, click **Configure System**, then click **Edit Disk Partitions**. Choose the VMFS accessibility setting you want, then click **Save**.

Like most file systems, the VMFS file system does not have the ability to handle accesses by more than one server simultaneously. When a VMFS partition has its attribute set to public or shared, ESX Server automatically does appropriate locking whenever the VMFS file system is accessed. This locking ensures that the VMFS is not opened by more than one server at a time. If the attribute of the VMFS is set to private, ESX Server presumes that it cannot be accessed by more than one server at a time and does not do any locking.

When a VMFS file system is mounted as `/vmfs` on a particular server, the VMFS file system is opened and locked by that server. Therefore, no other server can access that VMFS file system. In particular, no other server can simultaneously mount that file system on `/vmfs`. Since only one server at a time can mount a public or shared VMFS on `/vmfs`, VMware ESX Server does not mount public or shared VMFS file systems on `/vmfs` by default when the system starts. ESX Server only mounts private VMFS file systems on `/vmfs` by default.

If you know that only a single server will ever access a particular VMFS file system on the SAN, you may explicitly mount that VMFS by executing a command such as:

```
mount-vmfs vmhba0:2:0:1
```

on that server. This `mount-vmfs` command may be put in a console operating system startup script, such as `/etc/rc.d/rc.local`. You can use `mount-vmfs` with the `-f` option, which will force the mounting of all VMFS partitions that are not already mounted by another server. See the `mount-vmfs(8)` man page for details.

If you receive an unexpected error via the management interface when doing a VMFS operation on a SAN disk, it may be because another server is accessing that VMFS partition. In particular, another server may have locked the VMFS partition by mounting the VMFS partition to `/vmfs`.

### Suspend Directory

You may set a virtual machine's suspend directory to a `/vmfs /...` path name, so that the virtual machine's suspended state file is written to a VMFS file system. Typically, suspending to a VMFS file system will provide faster performance. However, whenever

you prepare to suspend or resume the virtual machine, you must ensure that the appropriate VMFS file system is mounted on `/vmfs`.

This requirement does not typically cause problems for private file systems, since private VMFS file systems are always mounted at startup on `/vmfs`.

However, if you wish to suspend to a VMFS file system with accessibility set to public or shared, you must ensure that file system is mounted, possibly by issuing an explicit `mount-vmfs` command, as described above, and unmounting afterwards using `umount-vmfs`.

# 8

## Networking

## Networking

This section contains the following:

- [Setting the MAC Address Manually for a Virtual Machine on page 217](#)
  - [How VMware ESX Server Generates MAC Addresses on page 217](#)
  - [Setting MAC Addresses Manually on page 218](#)
- [The VMkernel Network Card Locator on page 220](#)
- [Forcing the Network Driver to Use a Specific Speed on page 221](#)
- [Sharing Network Adapters and Virtual Networks on page 224](#)
  - [Allowing the Console Operating System to Use the Virtual Machines' Devices on page 224](#)
  - [Starting Shared VMkernel Network Adapters and Virtual Networks when the Console Operating System Boots on page 225](#)
  - [Sharing the Console Operating System's Network Adapter with Virtual Machines on page 226](#)
- [Performance Tuning for Heavy Network Loads on page 228](#)
  - [Enabling Interrupt Clustering on page 228](#)
  - [Interrupt Clustering Parameters on page 228](#)



# Setting the MAC Address Manually for a Virtual Machine

VMware ESX Server automatically generates MAC addresses for the virtual network adapters in each virtual machine. In most cases, these MAC addresses are appropriate. However, there may be times when you need to set a virtual network adapter's MAC address manually — for example:

- You have more than 256 virtual network adapters on a single physical server.
- Virtual network adapters on different physical servers share the same subnet and are assigned the same MAC address, causing a conflict.
- You want to ensure that a virtual network adapter always has the same MAC address.

This document explains how VMware ESX Server generates MAC addresses and how you can set the MAC address for a virtual network adapter manually.

## How VMware ESX Server Generates MAC Addresses

Each virtual network adapter in a virtual machine gets its own unique MAC address. ESX Server attempts to ensure that the network adapters for each virtual machine that are on the same subnet have unique MAC addresses. The algorithm used by ESX Server puts a limit on how many virtual machines can be running and suspended at once on a given machine. It also does not handle all cases when virtual machines on distinct physical machines share a subnet.

A MAC address is a six-byte number. Each network adapter manufacturer gets a unique three-byte prefix called an OUI — organizationally unique identifier — that it can use to generate unique MAC addresses. VMware has two OUIs — one for automatically generated MAC addresses and one for manually set addresses.

The VMware OUI for automatically generated MAC addresses is 00:05:69. Thus the first three bytes of the MAC address that is automatically generated for each virtual network adapter have this value. ESX Server then uses a MAC address generation algorithm to produce the other three bytes. The algorithm guarantees unique MAC addresses within a machine and attempts to provide unique MAC addresses between ESX Server machines.

The algorithm that ESX Server uses is the following:

When the algorithm generates the last 24 bits of the MAC address, the first 16 bits are set to the same values as the last 16 bits of the console operating system's primary IP address.

The final eight bits of the MAC address are set to a hash value based on the name of the virtual machine's configuration file.

ESX Server keeps track of all MAC addresses that have been assigned to network adapters of running and suspended virtual machines on a given physical machine. ESX Server ensures that the virtual network adapters of all of these virtual machines have unique MAC addresses.

The MAC address of a powered-off virtual machine is not remembered. Thus it is possible that when a virtual machine is powered on again it can get a different MAC address.

For example, if a machine had IP address 192.34.14.81 (or in hex, 0xc0220e51) and the configuration file hashed to the value 95, the MAC address would have the following value:

```
00:05:69:0e:51:95
```

Since there are only eight bits that can vary for each MAC address on an ESX Server machine, this puts a limit of 256 unique MAC addresses per ESX Server machine. This in turn limits the total number of virtual network adapters in all powered-on and suspended virtual machines to 256. This limitation can be eliminated by using the method described in the section [Setting MAC Addresses Manually](#) (below).

**Note:** The use of parts of the console operating system's IP address as part of the MAC address is an attempt to generate MAC addresses that are unique across different ESX Server machines. However, there is no guarantee that different ESX machines with physical network adapters that share a subnet always generate mutually exclusive MAC addresses.

### Setting MAC Addresses Manually

In order to work around both the limit of 256 virtual network adapters per physical machine and possible MAC address conflicts between virtual machines, the MAC addresses can be assigned manually by system administrators. VMware uses a different OUI for manually generated addresses: 00:50:56. The addresses can be set by adding the following line to a virtual machine's configuration file:

```
ethernet0.address = 00:50:56:XX:YY:ZZ
```

where **XX** is a valid hex number between 00 and 3F and **YY** and **ZZ** are valid hex numbers between 00 and FF. The value for **XX** must not be greater than 3F in order to

avoid conflict with MAC addresses that are generated by the VMware Workstation and VMware GSX Server products. Thus the maximum value for a manually generated MAC address is

```
ethernet0.address = 00:50:56:3F:FF:FF
```

VMware ESX Server virtual machines do not support arbitrary MAC addresses, hence the above format must be used. So long as you choose `XX:YY:ZZ` so it is unique among your hard-coded addresses, conflicts between the automatically assigned MAC addresses and the manually assigned ones should never occur.

## The VMkernel Network Card Locator

When network interface cards are assigned to the VMkernel, sometimes it is difficult to map from the name of the VMkernel device to the physical network adapter on the machine.

For example, if there are four Intel EEPo cards in a machine and all are dedicated to the VMkernel, these four cards are called `vmnic0`, `vmnic1`, `vmnic2` and `vmnic3`. The name of a card is based on its order in the PCI bus/slot hierarchy on the machine — the lower the bus and slot, the lower the number at the end of the name.

If you know the bus and slot order of the adapters, you can figure out which adapter has which name. However, if you don't, you can use the `findnic` program to help you make the proper association of network adapter to name.

The format of the command is

```
findnic <options> <nic-name> <local-ip> <remote-ip>
```

The `findnic` program takes a VMkernel network device name, an IP address to give the device on the local machine and an IP address that `findnic` should try to ping. When you issue the command, `findnic` pings the remote IP address.

This allows you to determine which adapter is which by looking at the LEDs on the cards to see which one has flashing lights or by seeing if the ping itself is successful.

### Options

`-f`

Do a flood ping.

`-i <seconds>`

Interval in seconds between pings.

### Examples

```
findnic vmnic0 10.2.0.5 10.2.0.4
```

Binds VMkernel device `vmnic0` to IP address 10.2.0.5 and then tries to ping the remote machine with the IP address 10.2.0.4.

```
findnic -f vmnic1 10.2.0.5 10.2.0.4
```

Binds VMkernel device `vmnic1` to IP address 10.2.0.5 and then tries to flood ping the remote machine with the IP address 10.2.0.4.

## Forcing the Network Driver to Use a Specific Speed

The VMkernel network device drivers start with a default setting of 100Mbps, full duplex. This setting should work correctly with network switches set for 100Mbps, full duplex and with switches set to autonegotiate.

If you encounter problems — in particular, very low receive speeds — it is likely that your switch is set for 100Mbps, half duplex.

To resolve the problem, either change the settings on your switch or change the settings for the VMkernel network device using the VMware Management Interface.

1. Log in to the management interface as root.
2. Go to the Network Configuration page (**Configure System > Network Configuration**).
3. Locate the device you want to reconfigure and choose the appropriate setting from the drop-down list in the New Speed/Duplex column.
4. Click **Update Network Configuration**.

## Forcing a Virtual Adapter to Use Promiscuous Mode

For security reasons, guest operating systems are not normally allowed to set their virtual Ethernet adapters to use promiscuous mode.

In some circumstances, you may need to use the virtual Ethernet adapters in promiscuous mode. To enable this use, you must set the `PromiscuousAllowed` configuration variable to `yes`. To do so, follow these steps.

1. Check the Edit Configuration page of the VMware Management Interface to determine what network the virtual Ethernet adapter is using. For this example, assume that the Networking section of the page shows the adapter is using `vmnic0`.
2. Log in to the server's console operating system and enter the following command:

```
echo "PromiscuousAllowed yes" > /proc/vmware/net/vmnic0/config
```

This allows the guest operating systems in all virtual machines using `vmnic0` to enable promiscuous mode.

If the adapter is using a different network, such as `vmnet_0`, make the appropriate substitution in the command.

3. Take the appropriate steps in the guest operating system to enable promiscuous mode on the virtual network adapter.

You may want to allow only some adapters on a particular network to use promiscuous mode. In that case, you can selectively disable promiscuous mode based on the MAC address of the virtual machine's Ethernet adapter. To do so, follow these steps.

1. Connect to the virtual machine with the remote console and use the appropriate guest operating system tools to determine the MAC address of the virtual Ethernet adapter.
2. Log in to the console operating system and enter the following command:

```
echo "PromiscuousAllowed no" > /proc/vmware/net/vmnic0/<MACAddress>
```

In place of `<MACAddress>`, substitute the virtual Ethernet adapter's MAC address in the standard format `00:05:69:XX:YY:ZZ`. If the adapter is using

a different network, such as `vmnet_0`, make the appropriate substitution in the command.

## Sharing Network Adapters and Virtual Networks

In many ESX Server configurations, there is a clear distinction between networking resources used by the virtual machines and those used by the console operating system. This may be important for security reasons, for example — isolating the management network from the network used by applications in the virtual machines.

However, there may be times when you want to share resources, including physical network adapters and virtual networks.

This technical note provides instructions on sharing in both directions — making the virtual machines' resources available to the console operating system and allowing virtual machines to share the network adapter used by the console operating system.

This sharing is made possible by the `vmxnet_console` driver, which is installed with the console operating system.

**Caution:** We recommend that only advanced users make these configuration changes. The steps below are easier for someone who is familiar with administering a Linux system.

**Note:** If you accidentally bring down the local loopback interface while you are reconfiguring network devices, the VMware Management Interface does not function properly. To bring it back up, use the command `ifconfig lo up`.

### Allowing the Console Operating System to Use the Virtual Machines' Devices

All network adapters used by virtual machines (that is, assigned to the VMkernel) and virtual networks can be made accessible to the console operating system. Virtual networks — identified as `vmnet_<n>` on the Edit Configuration page of the VMware Management Interface — provide high-speed connections among virtual machines on the same physical server.

To give the console operating system access to VMkernel network adapters and virtual networks, you must install the `vmxnet_console` module. When you install it, you provide a list of VMkernel network adapters and virtual networks that the `vmxnet_console` module should attach to. For example, if the VMkernel had an adapter named `vmnic1` and a virtual network named `vmnet_0` and you wanted to



provide access to them from the console operating system, you would use the following command to install the `vmxnet_console` module.

```
insmod vmxnet_console devName=vmnic1,vmnet_0
```

The `devName` parameter is a comma-separated list of names of VMkernel network adapters and virtual networks.

When you install the module, it adds the appropriate number of `eth<n>` devices on the console operating system in the order that you list the VMkernel network adapter and virtual network names after the `devName` parameter. In the example above, if the console operating system already had a network adapter named `eth0`, when you load `vmxnet_console` with `vmnic1` and `vmnet_0`, `vmnic1` is seen as `eth1` on the console operating system and `vmnet_0` is seen as `eth2`.

Once the `eth<n>` devices are created on the console operating system, you can bring the interfaces up in the normal manner. For example, if you want the console operating system to use IP address 10.2.0.4 for the network accessed via the `vmnic1` adapter, use the following command:

```
ifconfig eth1 up 10.2.0.4
```

If you want an easy way to see which `eth<n>` devices are added by the `insmod` command, you can add the `tagName` parameter to the `insmod` command, as shown in this example:

```
insmod vmxnet_console devName=vmnic1,vmnet_0 tagName=<tag>
```

In this case the `vmxnet_console` module adds the names of each of the `eth<n>` devices that it created to `/var/log/messages`. Each message begins with the string `<tag>`. To figure out the names of the devices that were added, use this command:

```
grep <tag> /var/log/messages
```

## Starting Shared VMkernel Network Adapters and Virtual Networks when the Console Operating System Boots

There are two ways you can configure the console operating system to start VMkernel network adapters when the console operating system boots. The simpler case involves sharing a network adapter other than `eth0`. Sharing `eth0` is more complicated and is described later.

Continuing with the example from the previous section, you can append the following lines to `/etc/rc.d/rc.local`:

```
insmod vmxnet_console devName=vmnic1,vmnet_0
ifconfig eth1 up 10.2.0.4
ifconfig eth2 up 63.93.12.47
```

Another method is to set up the files `/etc/sysconfig/network-scripts/ifcfg-eth1` and `/etc/sysconfig/network-scripts/ifcfg-eth2` with the appropriate network information. And be sure the `ONBOOT=` line is `ONBOOT=yes`. The `ifcfg-eth1` file for this example would be

```
DEVICE=eth1
BOOTPROTO=static
BROADCAST=10.255.255.255
IPADDR=10.2.0.4
NETMASK=255.0.0.0
NETWORK=10.0.0.0
ONBOOT=yes
```

In this case, the lines you add to `/etc/rc.d/rc.local` would be:

```
insmod vmxnet_console devName=vmnic1,vmnet_0
ifup eth1
ifup eth2
```

### Sharing the Console Operating System's Network Adapter with Virtual Machines

**Caution:** If you intend to share the adapter that is `eth0` on the console operating system, be careful as you implement the following steps. In order to configure ESX Server initially, you need to have a network connection. Once the initial configuration is set, you make several changes. At one point in the process, there is no network connection to the console operating system, and you must work directly at the server.

When you first install and configure ESX Server, the VMkernel is not loaded, so the console operating system needs to control the network adapter that is `eth0`. When you configure ESX Server, assign the adapter that is `eth0` to the console operating system.

Once you have completely configured ESX Server properly and rebooted the machine, the VMkernel is loaded. At that point, you need to take the following steps:

1. Edit `/etc/modules.conf` and comment out the line that refers to `alias eth0`.

If the original line is

```
alias eth0 e100
```

edit it to be

```
# alias eth0 e100
```

This disables `eth0` on the console operating system when it boots.

2. Use the VMware Management Interface to reconfigure the server. Log in as root and go to `http://<hostname>/pcidivv`, then click the **Edit** link for the configuration you want to change. Find the table row that lists the Ethernet controller assigned to the console and click the radio button in the Virtual Machine column to reassign it.

Click **Save Configuration**, then reboot the machine when prompted.

3. When the machine reboots, no network adapter is assigned to the console operating system, so you must do this step at the server.

Add the appropriate lines to `/etc/rc.d/rc.local`. For example, if `eth0` is the only network adapter that you intend to share between the VMkernel and the console operating system, and if it is named `vmnic0` in the VMkernel, you add the lines

```
insmod vmxnet_console devName=vmnic_0
ifup eth0
```

If you are unsure what name the VMkernel has assigned to the network adapter that formerly was `eth0` in the console operating system, you can determine its name using the `findnic` program (see [The VMkernel Network Card Locator on page 220](#)).

4. The next time you reboot the system, the network adapter is shared by the console operating system and the virtual machines.

To begin sharing the network adapter without rebooting the system, you can manually issue the same commands you added to `/etc/rc.d/rc.local`.

```
insmod vmxnet_console devName=vmnic_0
ifup eth0
```

# Performance Tuning for Heavy Network Loads

If your virtual machines have heavy network loads composed of many connections, you may be able to improve performance by using the interrupt clustering feature of ESX Server.

Interrupt clustering allows ESX Server to consume less CPU time for inbound packets by handling many of them at once. You will need to experiment with the values for these parameters to determine the best settings for your configuration.

## Enabling Interrupt Clustering

Interrupt clustering is turned off by default. When you enable interrupt clustering, it takes effect for all virtual machines running on the server.

Use the VMware Management Interface to enable it. Log in to the management interface as root, click **Configure System**, then click **Network Configuration**. On the Network Configuration page, enable interrupt clustering, then follow the link to the VMkernel Configuration page, where you can adjust the parameters.

## Interrupt Clustering Parameters

### NetRXClusterThreshOn

This parameter specifies the interrupt rate at which the VMkernel should switch to polling mode. Once in polling mode, the network adapter no longer generates interrupts when packets arrive, and packets are handled at regular intervals specified by NetRXClusterTMaxFreq.

Lowering the value of this parameter can increase performance at higher traffic rates.

Raising the value of this parameter can increase performance at lower traffic rates.

Recommended range: 2000–20000

### NetRXClusterThreshOff

This parameter specifies the interrupt rate at which the VMkernel should switch back to interrupt mode. In interrupt mode, the network adapter will interrupt the VMkernel whenever a packet has arrived. The value of this parameter should be lower than NetRXClusterThreshOn. A value that is half of NetRXClusterThreshOn is a good starting point.

Lowering the value of this parameter can increase performance at higher traffic rates.

Raising the value of this parameter can increase performance at lower traffic rates.

Recommended range: 1000–10000

### **NetRXClusterDelayOn**

This parameter specifies how sensitive to changes in traffic rate the VMkernel is when it is in interrupt mode.

Lowering the value of this parameter causes the VMkernel to switch to polling mode faster in response to sudden increases in traffic rate.

Raising the value of this parameter causes the VMkernel to be more tolerant of erratic traffic rates.

Recommended range: 0–10

### **NetRXClusterDelayOff**

This parameter specifies how sensitive to changes in traffic rate the VMkernel is when it is in polling mode.

Lowering the value of this parameter causes the VMkernel to switch to interrupt mode faster in response to sudden decreases in traffic rate.

Raising the value of this parameter causes the VMkernel to be more tolerant of erratic traffic rates.

Recommended range: 10–30

### **NetRXClusterTMaxFreq**

The interrupt clustering feature relies on a periodic timer both for sampling the traffic rate and for processing received packets when the NIC is in polling mode. The value of this parameter specifies the frequency (as a power of 2) at which the network adapter is polled for packets when it is in polling mode.

Lowering the value of this parameter can increase performance in situations where traffic rates are high and the traffic is made up of connections to many different machines.

Raising the value of this parameter can increase performance in situations where traffic rates are low or the traffic is made up of connections to only a few machines.

Recommended range for 100Mb connections: 9–11

Recommended range for 1000Mb connections: 10–12

### **NetRXClusterTMinFreq**

The value of this parameter specifies the frequency (as a power of 2) at which the traffic rate is sampled when the network adapter is in interrupt mode.

Lowering the value of this parameter decreases the CPU overhead of the traffic rate sampling when the network adapter is in interrupt mode.

Raising the value of this parameter allows the VMkernel to react more quickly to sudden increases in traffic rate.

Recommended range: 4–6

### **NetRXClusterDelayTInc**

The value of this parameter specifies how quickly the VMkernel increases the sampling rate to NetRXClusterTMaxFreq when the network adapter is switched into polling mode.

Lowering the value of this parameter allows the VMkernel to react more quickly to sudden increases in traffic rate.

Raising the value of this parameter causes the VMkernel to be more tolerant of erratic traffic rates.

Recommended range: 0–10

### **NetRXClusterDelayTDec**

The value of this parameter specifies how quickly the VMkernel decreases the sampling rate to NetRXClusterTMinFreq when the network adapter is switched into polling mode.

Lowering the value of this parameter allows the VMkernel to react more quickly to sudden decreases in traffic rate.

Raising the value of this parameter causes the VMkernel to be more tolerant of erratic traffic rates.

Recommended range: 100–2000

# 9

## **Resource Management**

# Resource Management

This section contains the following:

- [CPU Resource Management on page 234](#)
  - [Proportional-share Scheduling on page 234](#)
  - [Multiprocessor Systems on page 235](#)
  - [Managing CPU Resources from the Management Interface on page 236](#)
  - [Managing CPU Resources from the Console Operating System on page 236](#)
- [Memory Resource Management on page 239](#)
  - [Allocation Parameters on page 239](#)
  - [Admission Control on page 240](#)
  - [Dynamic Allocation on page 240](#)
  - [Memory Reclamation on page 241](#)
  - [Memory Sharing on page 242](#)
  - [Managing Memory Resources from the Management Interface on page 243](#)
  - [Managing Memory Resources with Configuration File Settings on page 243](#)
  - [Console Operating System Commands on page 244](#)
- [Sizing Memory on the Server on page 249](#)
  - [Server Memory on page 249](#)
  - [Console Operating System Memory on page 249](#)
  - [Virtual Machine Memory Pool on page 249](#)
  - [Virtual Machine Memory on page 250](#)
  - [Memory Sharing on page 250](#)
  - [Memory Overcommitment on page 251](#)
  - [Example: Web Server Consolidation on page 251](#)
- [Network Bandwidth Management on page 253](#)
  - [Using Network Filters on page 253](#)
  - [Managing Network Bandwidth from the Management Interface on page 253](#)
  - [Managing Network Bandwidth from the Console Operating System on page 254](#)
  - [Traffic Shaping with nfshaper on page 254](#)



- [Disk Bandwidth Management on page 257](#)
  - [Managing Disk Bandwidth from the Management Interface on page 258](#)
  - [Managing Disk Bandwidth from the Console Operating System on page 259](#)

## CPU Resource Management

VMware ESX Server provides dynamic control over both the execution rate and the processor assignment of each scheduled virtual machine. The scheduler performs automatic load balancing on multiprocessor systems.

You can manage the CPU resources on a server from the VMware Management Interface or from the console operating system's command line.

### Proportional-share Scheduling

Proportional-share processor scheduling gives you intuitive control over execution rates. Each scheduled virtual machine is allocated a number of shares that entitle it to a fraction of processor resources. For example, a virtual machine that is allocated twice as many shares as another is entitled to consume twice as many CPU cycles. In general, a runnable virtual machine with  $S$  shares on a processor with an overall total of  $T$  shares is guaranteed to receive at least a fraction  $S/T$  of the processor CPU time.

For example, if you are running three virtual machines, each starts with a default allocation of 1,000 shares. If you want to give one virtual machine half the CPU time and give each of the other two virtual machines one-quarter of the CPU time, you can assign 2,000 shares to the first virtual machine and leave the other two at their default allocations. Since these share allocations are relative, the same effect may be achieved by giving 500 shares to the first virtual machine and 250 to each of the other two virtual machines.

You can control relative CPU rates by specifying the number of shares allocated to each virtual machine. The system automatically keeps track of the total number of shares,  $T$ . Increasing the number of shares allocated to a virtual machine dilutes the effective value of all shares by increasing  $T$ .

Absolute guarantees for minimum CPU rates can be specified by following the simple convention of limiting the total number of shares allocated across all virtual machines. For example, if the total number of shares is limited to 10,000 or less, each share represents a guaranteed minimum of at least 0.01 percent of processor CPU cycles.

The console operating system receives 1,000 shares by default. In most cases, this should be an appropriate allocation, since the console operating system should not be used for CPU-intensive tasks. If you do find it necessary to adjust the console operating system's allocation of CPU shares, you can use the `procfs` interface, as described in this section. Or you can achieve a similar result indirectly, using the VMware Management Interface, by adjusting the shares of the virtual machines

running on the server so the console operating system's 1,000 shares represent a greater or smaller proportion of the total.

Shares are not hard partitions or reservations, so underutilized allocations are not wasted. Instead, inactive shares are effectively removed from consideration, allowing active virtual machines to benefit when extra resources are available.

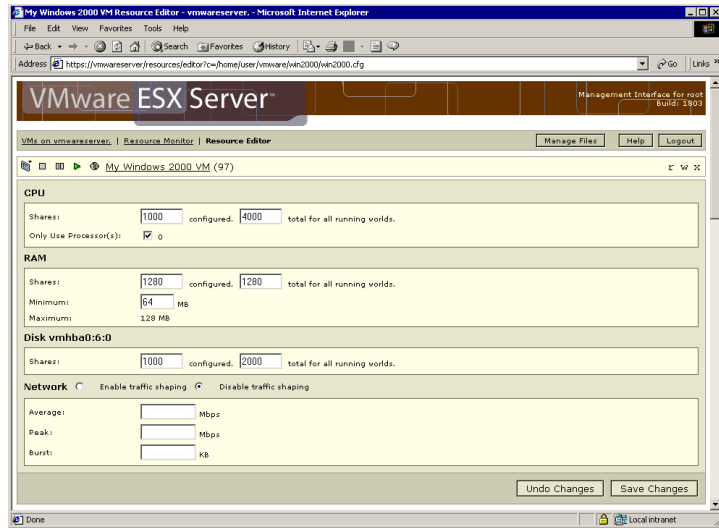
### **Multiprocessor Systems**

In multiprocessor systems, you can also restrict the assignment of virtual machines to a subset of the available processors by specifying an affinity set for each virtual machine. The system automatically assigns each virtual machine to a processor in the specified affinity set in order to balance the number of active shares across processors. If the affinity set contains only a single processor, then the virtual machine is placed there.

Any one virtual machine is assigned to only one processor. And the guest operating system sees a virtual machine with a single processor.

The current release allows CPU shares and affinity sets to be specified and modified dynamically at any time using a simple `procfs` interface or using the VMware Management Interface. Initial values for a virtual machine may also be specified in its configuration file.

### Managing CPU Resources from the Management Interface



You may also change settings from the Resource Editor page of the VMware Management Interface. On the server's Overview page, click **Manage Resources**. The Resource Monitor page appears. Click **Edit Resources** under the name of the virtual machine for which you want to change settings. Enter the desired settings, then click **Save Changes**.

You must log in as root in order to change resource management settings using either the management interface or `procs`.

### Managing CPU Resources from the Console Operating System

`sched.cpu.shares = <nshares>`

This configuration file option specifies the initial share allocation for a virtual machine as `<nshares>` shares. The valid range of values for `<nshares>` is 1 to 100000, enabling a large range of allocation ratios. The default allocation is 1,000 shares.

`sched.cpu.affinity = <set>`

This configuration file option specifies the initial processor affinity set for a virtual machine. If `<set>` is `all` or `default`, then the affinity set contains all available processors. The specified set may also be a comma-separated list of CPU numbers such as `0, 2, 3`.

```
/proc/vmware/vm/<id>/cpu/shares
```

Reading from this file reports the number of shares allocated to the virtual machine identified by <id>.

Writing a number <nshares> to this file changes the number of shares allocated to the virtual machine identified by <id> to <nshares>. The valid range of values for <nshares> is 1 to 100000.

```
/proc/vmware/vm/<id>/cpu/affinity
```

Reading from this file reports the number of each CPU in the current affinity set for the virtual machine identified by <id>.

Writing a comma-separated list of CPU numbers to this file, such as 0, 2, 3, changes the affinity set for the virtual machine identified by <id>. Writing **all** or **default** to this file changes the affinity set to contain all available processors.

```
/proc/vmware/vm/<id>/cpu/status
```

Reading from this file reports current status information for the virtual machine identified by <id>, including the specified shares and affinity parameters, as well as the virtual machine name, state (running, ready, waiting), current CPU assignment and cumulative CPU usage in seconds.

```
/proc/vmware/sched/cpu.<n>
```

Reading from this file reports the status information for all active virtual machines currently assigned to cpu number <n>, as well as some aggregate totals.

```
/proc/vmware/sched/cpu
```

Reading from this file reports the status information for all virtual machines in the entire system.

```
/proc/vmware/config/CpuBalancePeriod
```

This ESX Server option specifies the periodic time interval, in seconds, for automatic multiprocessor load balancing based on active shares. Defaults to 1 second.

### Examples

Suppose that we are interested in the CPU allocation for the virtual machine with ID 103. To query the number of shares allocated to virtual machine 103, simply read the file.

```
cat /proc/vmware/vm/103/cpu/shares
```

The number of shares is displayed.

```
1000
```

This indicates that virtual machine 103 is currently allocated 1,000 shares. To change the number of shares allocated to virtual machine 103, simply write to the file. Note that you need root privileges in order to change share allocations.

```
echo 2000 > /proc/vmware/vm/103/cpu/shares
```

The change can be confirmed by reading the file again.

```
cat /proc/vmware/vm/103/cpu/shares
```

The number of shares is displayed.

```
2000
```

To query the affinity set for virtual machine 103, simply read the file:

```
cat /proc/vmware/vm/103/cpu/affinity
```

The identifying numbers of the processors in the affinity set are displayed.

```
0,1
```

This indicates that virtual machine 103 is allowed to run on CPUs 0 and 1. To restrict virtual machine 103 to run only on CPU 1, simply write to the file. Note that you need root privileges in order to change affinity sets.

```
echo 1 > /proc/vmware/vm/103/cpu/affinity
```

The change can be confirmed by reading the file again.

### Cautions

CPU share allocations do not necessarily guarantee the rate of progress within a virtual machine. For example, suppose virtual machine 103 is allocated 2,000 shares, while virtual machine 104 is allocated 1,000 shares. If both virtual machines are CPU-bound — for example, both are running the same compute-intensive benchmark — then virtual machine 103 should indeed run twice as fast as virtual machine 104. However, if virtual machine 103 instead runs an I/O-bound workload that causes it to stop as it waits for other resources, it does not run twice as fast as virtual machine 103, even though it is allowed to use twice as much CPU time.

## Memory Resource Management

VMware ESX Server provides dynamic control over the amount of physical memory allocated to each virtual machine. You may overcommit memory, if you wish, so the total size configured for all running virtual machines exceeds the total amount of available physical memory. The system manages the allocation of memory to virtual machines automatically based on allocation parameters and system load.

You may specify initial memory allocation values for a virtual machine in its configuration file. You may also modify most memory allocation parameters dynamically using the VMware Management Interface, the `procfs` interface on the console operating system or the Perl API. Reasonable defaults are used automatically when parameters are not specified explicitly.

You have access to information about current memory allocations and other status information through the management interface, the `procfs` interface on the console operating system and the Perl API.

### Allocation Parameters

Three basic parameters control the allocation of memory to each virtual machine:

- Its minimum size — `min`
- Its maximum size — `max`
- Its shares allocation

The system automatically allocates an amount of memory to each virtual machine somewhere between its minimum and maximum sizes based on its shares and an estimate of its recent working set size.

The maximum size is the amount of memory configured for use by the guest operating system running in the virtual machine. This maximum size must be specified in the configuration file for the virtual machine. By default, virtual machines operate at their maximum allocation, unless memory is overcommitted.

The minimum size is a guaranteed lower bound on the amount of memory that is allocated to the virtual machine, even when memory is overcommitted. The system uses an admission control policy to enforce this guarantee. A new virtual machine is not permitted to power on if there is insufficient memory to reserve its minimum size.

Memory shares entitle a virtual machine to a fraction of physical memory. For example, a virtual machine that has twice as many shares as another is generally entitled to consume twice as much memory, subject to their respective minimum

and maximum constraints, provided they are both actively using the memory they have been allocated.

### Admission Control

VMware ESX Server uses an admission control policy to ensure that sufficient unreserved memory and swap space are available before powering on a virtual machine. Memory must be reserved for the virtual machine's guaranteed minimum size; additional overhead memory is required for virtualization. Thus the total required for each virtual machine is the specified minimum plus overhead.

The overhead memory size is determined automatically; it is typically 32MB per virtual machine. Additional overhead memory is reserved for virtual machines larger than 1GB.

Swap space must be reserved on disk for the remaining virtual machine memory — that is the difference between the maximum and minimum settings. This swap reservation is required to ensure the system is able to preserve virtual machine memory under any circumstances. In practice, only a small fraction of the swap space may actually be used.

Similarly, while memory reservations are used for admission control, actual memory allocations vary dynamically, and unused reservations are not wasted.

The amount of swap space configured for the system limits the maximum level of overcommitment. A default swap file size equal to the physical memory size of the computer is recommended in order to support a reasonable 2x level of memory overcommitment. You may configure larger or smaller swap files. If you do not configure a swap file, memory may not be overcommitted. The swap file may be configured using the management interface or from the console operating system using the `vmkfstools` program. For details on `vmkfstools` see [Using vmkfstools on page 199](#).

### Dynamic Allocation

Virtual machines are allocated their maximum memory size unless memory is overcommitted. When memory is overcommitted, each virtual machine is allocated an amount of memory somewhere between its minimum and maximum sizes. The amount of memory granted to a virtual machine above its minimum size may vary with the current memory load. The system automatically determines allocations for each virtual machine based on two factors: the number of shares it has been given and an estimate of its recent working set size.

VMware ESX Server uses a modified proportional-share memory allocation policy. Memory shares entitle a virtual machine to a fraction of physical memory. For



example, a virtual machine that has twice as many shares as another is entitled to consume twice as much memory, subject to their respective minimum and maximum constraints, provided that they are both actively using the memory they have been allocated. In general, a virtual machine with  $S$  memory shares in a system with an overall total of  $T$  shares is entitled to receive at least a fraction  $S/T$  of physical memory.

However, virtual machines that are not actively using their currently allocated memory automatically have their effective number of shares reduced, in order to prevent virtual machines from unproductively hoarding idle memory. This is achieved by levying a tax on idle memory. A virtual machine is charged more for an idle page than for one that it is actively using.

The `MemIdleTax` configuration option provides explicit control over the policy for reclaiming idle memory. A tax rate of  $x$  percent means that up to  $x$  percent of a virtual machine's idle memory may be reclaimed. A low tax rate mostly ignores working sets and allocate memory based on shares. A high tax rate allows most idle memory to be reallocated away from virtual machines that are unproductively hoarding it, regardless of shares.

ESX Server estimates the working set for a virtual machine automatically by monitoring memory activity over successive periods of virtual machine virtual time. Estimates are smoothed over several periods using techniques that respond rapidly to increases in working set size and more slowly to decreases in working set size. This approach ensures that a virtual machine from which idle memory has been reclaimed is be able to ramp up quickly to its full share-based allocation once it starts using its memory more actively. The default monitoring period may be modified via the `MemSamplePeriod` configuration option.

### Memory Reclamation

ESX Server employs two distinct techniques for dynamically expanding or contracting the amount of memory allocated to virtual machines — a VMware-supplied `vmtoolsd` module that is loaded into the guest operating system running in a virtual machine and swapping pages from a virtual machine to a server swap file without any involvement by the guest operating system.

The preferred mechanism is the `vmtoolsd` driver, which cooperates with the server to reclaim those pages that are considered least valuable by the guest operating system. This proprietary technique provides predictable performance that closely matches the behavior of a native system under similar memory constraints. It effectively increases or decreases memory pressure on the guest operating system, causing the guest to invoke its own native memory management algorithms. When memory is tight, the guest operating system decides which particular pages to

reclaim and, if necessary, swaps them to its own virtual disk. The guest operating system must be configured with sufficient swap space. Some guest operating systems have additional limitations. See the notes in [Managing Memory Resources with Configuration File Settings on page 243](#) for details. If necessary, you can limit the amount of memory reclaimed using `vmxmemctl` by setting the `sched.mem.maxmemctl` option in the configuration file.

Swapping is used to forcibly reclaim memory from a virtual machine when no `vmxmemctl` driver is available. This may be the case if the `vmxmemctl` driver was never installed, has been explicitly disabled, is not running (for example, while the guest operating system is booting) or is temporarily unable to reclaim memory quickly enough to satisfy current system demands. Standard demand paging techniques swap pages back in when the virtual machine needs them.

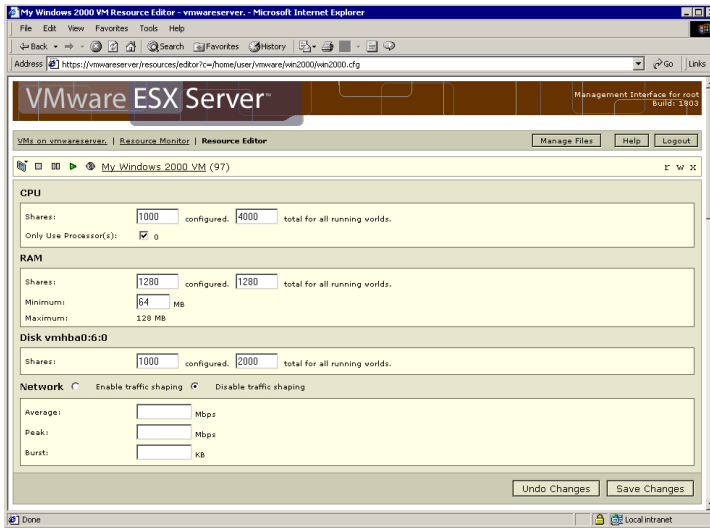
The `vmxmemctl` approach is used whenever possible for optimum performance. Swapping is a reliable mechanism of last resort that the system uses to reclaim memory only when necessary.

### Memory Sharing

Many ESX Server workloads present opportunities for sharing memory across virtual machines. For example, several virtual machines may be running instances of the same guest operating system, have the same applications or components loaded, or contain common data. In such cases, ESX Server uses a proprietary transparent page sharing technique to securely eliminate redundant copies of memory pages. With memory sharing, a workload running in virtual machines often consumes less memory than it would when running on physical machines. As a result, higher levels of overcommitment can be supported efficiently.

The ESX Server approach does not require any cooperation from the guest operating. You may use the `MemShareScanVM` and `MemShareScanTotal` configuration options to control the rate at which the system scans memory to identify opportunities for sharing memory.

### Managing Memory Resources from the Management Interface



On the server's Overview page, click **Manage Resources**. The Resource Monitor page appears. Click **Edit Resources** under the name of the virtual machine for which you want to change settings. Enter the desired settings, then click **Save Changes**.

You must log in as root in order to change resource management settings using either the management interface or `procfs`.

### Managing Memory Resources with Configuration File Settings

You can also manage memory resources by editing the following settings in the virtual machine's configuration file. To edit the configuration file, use the configuration file editor in the management interface. See [Editing a Virtual Machine's Configuration Remotely on page 99](#) for details.

```
memsize = <size>
```

This configuration file option specifies the maximum virtual machine size to be <size>MB.

```
sched.mem.minsize = <size>
```

This configuration file option specifies the guaranteed minimum virtual machine size to be <size>MB. The maximum valid value for <size> is 100 percent of the specified maximum virtual machine size. The minimum valid value for <size>

depends on the amount of available swap space. The default minimum size is 50 percent of the specified maximum virtual machine size.

`sched.mem.shares = <nshares>`

This configuration file option specifies the initial memory share allocation for a virtual machine to be `<nshares>` shares. The valid range of values for `<nshares>` is 0 to 100000, enabling a large range of allocation ratios. The default allocation is 10 times the maximum virtual machine size in megabytes.

`sched.mem.maxmemctl = <size>`

This configuration file option specifies the maximum amount of memory that may be reclaimed from the virtual machine using `vmxmemctl` to be `<size>`MB. If additional memory needs to be reclaimed, the system swaps instead of using `vmxmemctl`. The default maximum size is half of the specified maximum virtual machine size.

### Console Operating System Commands

`/proc/vmware/vm/<id>/mem/min`

Reading from this file reports the minimum memory size in megabytes for the virtual machine identified by `<id>`.

Writing a number `<size>` to this file changes the minimum memory size for the virtual machine identified by `<id>` to `<size>`MB.

`/proc/vmware/vm/<id>/mem/shares`

Reading from this file reports the number of memory shares allocated to the virtual machine identified by `<id>`.

Writing a number `<nshares>` to this file changes the number of memory shares allocated to the virtual machine identified by `<id>` to `<nshares>`. The valid range of values for `<nshares>` is 0 to 100000. Note that a value of zero shares causes the virtual machine memory size allocation to be exactly equal to its specified minimum size, even if excess memory is available.

`/proc/vmware/vm/<id>/mem/status`

Reading from this file reports current status information for the virtual machine identified by `<id>`, including the specified shares, minimum size and maximum size parameters as well as the virtual machine name, current status, whether the virtual machine is currently waiting for memory to be reserved, current memory usage, current target size, memory overhead for virtualization and the amount of allocated memory actively in use. All memory sizes are reported in kilobytes.

`/proc/vmware/sched/mem`

Reading from this file reports the memory status information for all nonsystem virtual machines in the entire system as well as several aggregate totals.

Writing the string `realloc` to this file causes an immediate memory reallocation. Memory is normally reallocated periodically every `MemBalancePeriod` seconds. (See `/proc/vmware/config/MemBalancePeriod` below for more information.) Reallocations are also triggered by significant changes in the amount of free memory.

`/proc/vmware/mem`

Reading from this file reports the maximum size with which a new virtual machine can be powered on, admission control status including the amount of unreserved memory and unreserved swap space, and the current amount of free memory in the system.

`/proc/vmware/pshare/status`

Reading from this file reports various detailed statistics about the current status of transparent page sharing.

`/proc/vmware/config/MemBalancePeriod`

This ESX Server option specifies the periodic time interval, in seconds, for automatic memory reallocations. Reallocations are also triggered by significant changes in the amount of free memory. The default is 15 seconds.

`/proc/vmware/config/MemSamplePeriod`

This ESX Server option specifies the periodic time interval, measured in seconds of virtual machine virtual time, over which memory activity is monitored in order to estimate working set sizes. The default is 30 seconds.

`/proc/vmware/config/MemIdleTax`

This ESX Server option specifies the idle memory tax rate as a percentage. This tax effectively charges virtual machines more for idle memory than for memory that they are actively using. A tax rate of 0 percent defines an allocation policy that ignores working sets and allocates memory strictly based on shares. A high tax rate results in an allocation policy that allows idle memory to be reallocated away from virtual machines that are unproductively hoarding it. The default is 75 percent.

`/proc/vmware/config/MemShareScanVM`

This ESX Server option specifies the maximum per-virtual machine rate at which memory should be scanned for transparent page sharing opportunities. The rate is specified as the number of pages to scan per second. The default is 50 pages per second per virtual machine.

`/proc/vmware/config/MemShareScanTotal`

This ESX Server option specifies the total systemwide rate at which memory should be scanned for transparent page sharing opportunities. The rate is specified as the number of pages to scan per second. The default is 200 pages per second.

`/proc/vmware/config/MemCtlMaxPercent`

This ESX Server option limits the maximum amount of memory that may be reclaimed from any virtual machine using `vmmemctl`, based on a percentage of its maximum size. Specifying 0 effectively disables reclamation via `vmmemctl` for all virtual machines. Defaults to 50.

`/proc/vmware/config/MemCtlMax[OSType]`

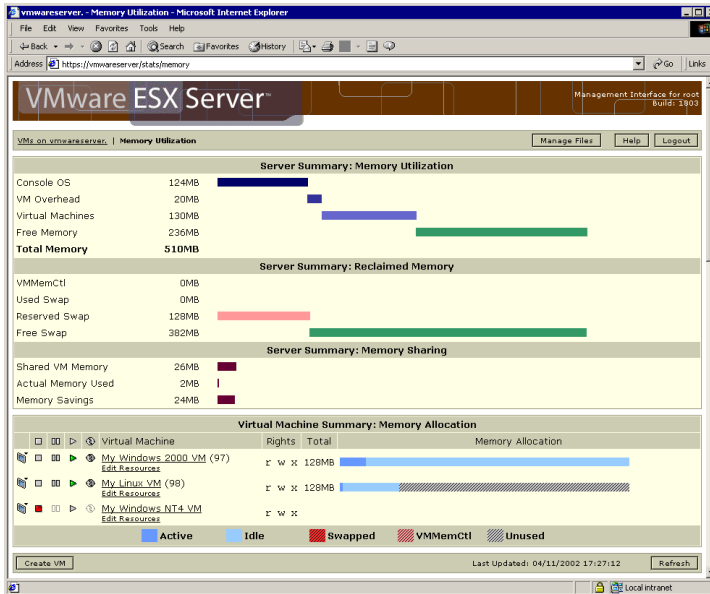
These ESX Server options restrict the maximum amount of memory that may be reclaimed from a virtual machine using `vmmemctl`, based on the limitations of guest operating system type. The value is specified in megabytes. Defaults to 128 for `OSType=NT4` (Windows NT 4.0), 2048 for `OSType=NT5` (Windows 2000 or .NET Server), 768 for `OSType=Linux` and 256 for `OSType=BSD`.

`/proc/vmware/config/MemCtlTimeout`

This ESX Server option specifies the time period, in seconds, after which a warning is logged for a virtual machine that has not yet started running `vmmemctl`. The default is 0 (disabled).

### Monitoring Memory Statistics

The Memory Utilization page in the VMware Management Interface provides information on the current use of RAM by the physical computer and the virtual machines running on it — in graphical and numerical form. To view this information, from the overview page click **Configure System**, then click **Memory Utilization**.



The Server Summary section at the top shows systemwide information. The Virtual Machine Summary section below it shows information for particular virtual machines. A detailed explanation of the information is at the bottom of the page.

You can also read the current memory statistics for a virtual machine from its status file on the console operating system. For example, to view the statistics for the virtual machine with ID 103, give this command:

```
cat /proc/vmware/vm/103/mem/status
```

The results are displayed in the following format:

```
vm      mctl?  wait  shares    min      max      size/sizetgt
103     yes    no    2560      131072   262144   217300/ 217300

memctl/mctltgt  swapped/swaptgt  shared  active  overhd/ovhdmax
39168/ 39168    5672/ 5672      38164  191756  14508/ 32768
```

The output above is shown with additional line breaks, in order to avoid wrapping long lines. All memory sizes are reported in kilobytes; 1 megabyte = 1024KB. The columns indicate:

`vm`                      virtual machine identifier

<code>mct1?</code>	<code>vmmemct1</code> driver active?
<code>wait</code>	blocked in a memory wait state?
<code>shares</code>	memory shares associated with the virtual machine
<code>min</code>	minimum size
<code>max</code>	maximum size
<code>size</code>	current size
<code>sizetgt</code>	target size
<code>memct1</code>	currently reclaimed using <code>vmmemct1</code>
<code>mct1tgt</code>	target to reclaim using <code>vmmemct1</code>
<code>swapped</code>	currently swapped to VMFS swap file
<code>swaptgt</code>	target to swap to VMFS swap file
<code>shared</code>	memory shared via transparent page sharing
<code>active</code>	current working set estimate
<code>overhd</code>	current overhead memory size
<code>ovhdmax</code>	maximum overhead memory size

In this example, the virtual machine with ID 103 is running the `vmmemct1` driver and is not currently blocked waiting for memory. The virtual machine is configured to use between 128MB and 256MB and has been allocated 2560 memory shares. It is currently allocated about 212MB. Approximately 44MB has been reclaimed for use by other virtual machines — 38MB via `vmmemct1` and nearly 6MB via swapping to the ESX server swap file. Of the 212MB allocated to the virtual machine, more than 37MB is shared — for example with other virtual machines. The current working set estimate for the virtual machine is approximately 187MB. About 14MB of overhead memory is currently being used for virtualization, out of a maximum of 32MB.

### Cautions

VMware supplies `vmmemct1` drivers for Windows XP, Windows 2000, Windows NT 4.0, Linux and FreeBSD. The appropriate `vmmemct1` driver is installed automatically when you install VMware Tools in the guest operating system. The system uses swapping to reclaim memory from virtual machines running other guest operating systems and from virtual machines that do not have VMware Tools installed.

The maximum amount of memory that the system may attempt to reclaim using `vmmemct1` is restricted automatically based on known limitations of the guest operating system type. Older versions of the `vmmemct1` driver do not support this feature; you should upgrade the driver to the current version. Alternatively, you may specify the configuration file option `sched.mem.maxmemct1` manually. See the description of the ESX Server option `MemCt1Max [OSType]` for appropriate limits.



## Sizing Memory on the Server

These guidelines are intended to help system administrators determine an appropriate amount of hardware memory for running a virtual machine workload on ESX Server 1.5. Since the characteristics of your particular workload also influence memory needs, you should follow up with testing to confirm that memory sizes computed according to these guidelines achieve the desired results.

ESX Server uses a small amount of memory for its own virtualization layer, additional memory for the console operating system and all remaining memory for running virtual machines. The sections below explain each of these uses and provide a quantitative sizing example.

### Server Memory

ESX Server 1.5 uses approximately 24MB of system memory for its own virtualization layer. This memory is allocated automatically when the ESX Server is loaded and is not configurable.

### Console Operating System Memory

The recommended amount of memory to configure for the console operating system varies between 128MB and 512MB, depending on the number of virtual machines you plan to run concurrently on the server:

- 128MB for  $\leq 4$  virtual machines
- 192MB for  $\leq 8$  virtual machines
- 272MB for  $\leq 16$  virtual machines
- 384MB for  $\leq 32$  virtual machines
- 512MB for  $> 32$  virtual machines

### Virtual Machine Memory Pool

The remaining pool of system memory is used for running virtual machines. ESX Server manages the allocation of this memory to virtual machines automatically based on administrative parameters and system load. ESX Server also attempts to keep some memory free at all times in order to handle dynamic allocation requests efficiently. ESX Server sets this level at approximately 6 percent of the memory available for running virtual machines.

### Virtual Machine Memory

Each virtual machine consumes memory based on its configured size, plus additional overhead memory for virtualization.

The dynamic memory allocation for a virtual machine is bounded by its minimum and maximum size parameters. The maximum size is the amount of memory configured for use by the guest operating system running in the virtual machine. By default, virtual machines operate at their maximum allocation, unless memory is overcommitted.

The minimum size is a guaranteed lower bound on the amount of memory that is allocated to the virtual machine, even when memory is overcommitted. The minimum size should be set to a level that ensures the virtual machine has sufficient memory to run efficiently, without excessive paging.

The maximum size can be set to a higher level to allow the virtual machine to take advantage of excess memory, when available.

Overhead memory includes space reserved for the virtual machine frame buffer and various virtualization data structures. A virtual machine configured with less than 1GB of memory requires 32MB of overhead memory. Larger virtual machines require an additional 4MB of overhead memory per additional gigabyte of configured main memory. For example, a virtual machine with a configured maximum memory size of 2GB requires 36MB of overhead memory.

### Memory Sharing

Many workloads present opportunities for sharing memory across virtual machines. For example, several virtual machines may be running instances of the same guest operating system, have the same applications or components loaded or contain common data. ESX Server uses a proprietary transparent page sharing technique to securely eliminate redundant copies of memory pages.

With memory sharing, a workload consisting of multiple virtual machines often consumes less memory than it would when running on physical machines. As a result, the system can support higher levels of overcommitment efficiently.

The amount of memory saved by memory sharing is highly dependent on workload characteristics. A workload consisting of many nearly-identical virtual machines may free up more than 30 percent of memory, while a more diverse workload may result in savings of less than 5 percent of memory.

To determine the effectiveness of memory sharing for a given workload, try running the workload, and observe the actual savings via the VMware Management Interface. The amount of memory shared and the associated savings are reported on the

Memory Utilization page (**Overview > Configure System > Memory Utilization**; you must be logged in as root to see this page).

ESX Server memory sharing runs as a background activity that scans for sharing opportunities over time. The amount of memory saved may vary over time; for a fairly constant workload, the amount generally increases slowly until all sharing opportunities are exploited.

### Memory Overcommitment

In many consolidated workloads, it is rare for all virtual machines to be actively using all of their memory simultaneously. Typically, some virtual machines are lightly loaded, while others are more heavily loaded, and relative activity levels generally vary over time. In such cases, it may be reasonable to overcommit memory to reduce hardware memory requirements.

ESX Server automatically transfers memory from idle virtual machines to virtual machines that actively need more memory in order to improve memory utilization.

You may also specify configuration parameters to preferentially devote space to important virtual machines.

The minimum size for a virtual machine defines a guaranteed lower bound on the amount of memory that it is allocated, even when memory is overcommitted. You can also use memory shares to specify the relative importance of different virtual machines. In any case, you should configure an appropriate minimum size for each virtual machine to ensure that each virtual machine can function effectively (without excessive paging), even when all virtual machines are active concurrently.

When memory is scarce, ESX Server dynamically reclaims space from some virtual machines based on importance and current working sets. For optimal performance, the server attempts to reclaim memory from a virtual machine via a VMware-supplied `vmtoolsd` module running in the guest. This allows the guest operating system to invoke its own native memory management policies, causing it to swap to its own virtual disk only when necessary.

ESX Server also has its own swap file and may also swap memory from a virtual machine to the ESX Server swap file directly, without any involvement by the guest operating system.

### Example: Web Server Consolidation

Suppose that you are using ESX Server to consolidate eight nearly-identical Web servers running IIS on Windows 2000. Each Windows 2000 machine is configured with

512MB of memory. The native memory requirement with eight physical servers is  $8 * 512\text{MB} = 4\text{GB}$ .

To consolidate these servers as virtual machines, 24MB is needed for the server virtualization layer and 192MB is recommended for the console operating system. Each virtual machine also requires an additional 32MB of overhead memory. An additional 6 percent should be added to account for the minimum free memory level. Assuming no overcommitment and no benefits from memory sharing, the memory required for virtualizing the workload is  $24\text{MB} + 192\text{MB} + (1.06 * 8 * (512\text{MB} + 32\text{MB})) = 4829\text{MB}$ . The total overhead for virtualization in this case is 733MB.

If memory sharing achieves a 10 percent savings (410MB), the total memory overhead drops to only 323MB. If memory sharing achieves a 25 percent savings (1GB), the virtualized workload actually consumes 291MB less memory than it would on eight physical servers.

It may also make sense to overcommit memory. For example, suppose that on average, two of the eight Web server virtual machines are typically idle and that each Web server virtual machine requires only 256MB to provide minimally acceptable service. In this case, the hardware memory size can be reduced safely by an additional  $2 * 256\text{MB} = 512\text{MB}$ . In the worst case where all virtual machines happen to be active at the same time, the system may need to swap some virtual machine memory to disk.

### More Information

For additional background information on ESX Server memory usage, see [Memory Resource Management on page 239](#).

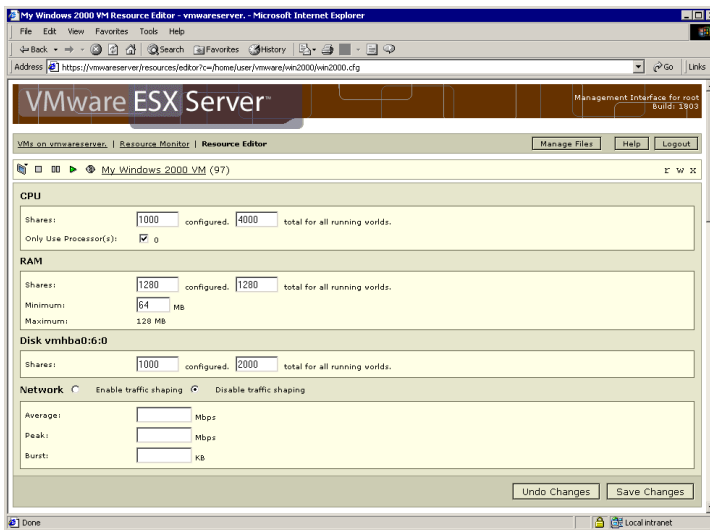
## Network Bandwidth Management

VMware ESX Server supports network traffic shaping with the `nfshaper` loadable module. A loadable packet filter module defines a filter class; multiple filter instances may be active for each loaded class. The current release supports only one filter class — `nfshaper`, which is a transmit filter for outbound bandwidth management that can be attached to virtual machines using either a `procs` interface or the VMware Management Interface.

### Using Network Filters

This section describes how to attach, detach and query filter instances from the console operating system's command line. You can also use the VMware Management Interface to attach and detach `nfshaper` and obtain statistics from it.

### Managing Network Bandwidth from the Management Interface



On the server's Overview page, click **Manage Resources**. The Resource Monitor page appears. Click **Edit Resources** under the name of the virtual machine for which you want to change settings. Enter the desired settings, then click **Save Changes**.

You must log in as root in order to change resource management settings using either the management interface or `procs`.

### Managing Network Bandwidth from the Console Operating System

`/proc/vmware/filters/status`

This file contains network filtering status information, including a list of all available filter classes and, for each virtual machine with attached filters, its list of attached filter instances. Read the file with `cat` to see a quick report on network filtering status.

`/proc/vmware/filters/xmitpush`

Command file used to add a new transmit filter instance to a virtual machine. Writing `<id> <class> [<args>]` to this file attaches a new instance of filter `<class>` instantiated with `<args>` to the virtual machine identified by `<id>`.

`/proc/vmware/filters/xmitpop`

Command file used to detach a transmit filter from a virtual machine. Writing `<id>` to this file detaches the last filter attached to the virtual machine identified by `<id>`.

`/proc/vmware/filters/xmit`

This directory contains a file for each active filter instance. Each file named `<class.n>` corresponds to the `<n>`th instance of filter class `<class>`.

Reading from a file reports status information for the filter instance in a class-defined format. Writing to a file issues a command to the filter instance using a class-defined syntax.

**Note:** The current release allows only a single network packet filter to be attached to each virtual machine. Receive filters are not implemented in this release.

### Traffic Shaping with `nfshaper`

You can manage network bandwidth allocation on a server from the VMware Management Interface or from the console operating system's command line.

Using a Web browser, you may change settings from the Resource Editor page of the management interface. Be sure the virtual machine you want to change is powered on. Then, on the server's Overview page, click **Manage Resources**. The Resource Monitor page appears. Click **Edit Resources** under the name of the virtual machine for which you want to change settings. Enter the desired settings, then click **Save Changes**.

You must log in as root in order to change resource management settings using either the management interface or the command line.

The shaper implements a two-bucket composite traffic shaping algorithm. A first token bucket controls sustained average bandwidth and burstiness. A second token

bucket controls peak bandwidth during bursts. Each `nfshaper` instance can accept parameters to control average bps, peak bps and burst size.

The `procfs` interface described in [Using Network Filters](#) is used to attach an `nfshaper` instance to a virtual machine, detach an `nfshaper` instance from a virtual machine, query the status of an `nfshaper` instance or issue a dynamic command to an active `nfshaper` instance.

### Commands

```
config <bpsAverage> <bpsPeak> <burstSize> [<periodPeak>]
```

Dynamically reconfigure the shaper to use the specified parameters: average bandwidth of `<bpsAverage>` bits per second, peak bandwidth of `<bpsPeak>` bits per second, maximum burst size of `<burstSize>` bytes and an optional peak bandwidth enforcement period `<periodPeak>` in milliseconds. Each parameter may optionally use the suffix k (1k = 1024) or m (1m = 1024k).

```
maxq <nPackets>
```

Dynamically set the maximum number of queued packets to `<nPackets>`.

```
reset
```

Dynamically reset shaper statistics.

### Examples

Suppose that you want to attach a traffic shaper to limit the transmit bandwidth of the virtual machine with ID 104. To create and attach a new shaper instance, issue an `xmitpush` command as described in [Using Network Filters on page 253](#). Note that root privileges are required to attach a filter.

```
echo "104 nfshaper 1m 2m 160k" > \
/proc/vmware/filters/xmitpush
```

This attaches a traffic shaper with average bandwidth of 1Mbps, peak bandwidth of 2Mbps and maximum burst size of 160Kb.

**Note:** This command should be entered on a single line. Do not type the backslash.

To find the number of the attached `nfshaper` instance, query the network filtering status, which contains a list of all filters attached to virtual machines:

```
cat /proc/vmware/filters/status
```

Suppose the reported status information indicates that the filter attached to virtual machine 104 is `nfshaper.2.104`. The `procfs` node for this filter can be used to obtain status information:

```
cat /proc/vmware/filters/xmit/nfshaper.2.104
```

The same `procs` node can also be used to issue commands supported by the `nfshaper` class. For example, you can dynamically adjust the bandwidth limits by issuing a `config` command:

```
echo "config 128k 256k 20k"> \  
/proc/vmware/filters/xmit/nfshaper.2.104
```

**Note:** This command should be entered on a single line. Do not type the backslash.

When a virtual machine is terminated, all attached network filters are automatically removed and destroyed. To manually remove a shaper instance you can issue an `xmitpop` command as described in [Using Network Filters on page 253](#). Note that root privileges are required to detach a filter.

```
echo "104" > /proc/vmware/filters/xmitpop
```



## Disk Bandwidth Management

ESX Server provides dynamic control over the relative amount of disk bandwidth allocated to each virtual machine. You can control disk bandwidth separately for each disk. The system manages the allocation of disk bandwidth to virtual machines automatically based on allocation parameters and system load. This is done in a way that maintains fairness and tries to maximize throughput.

You may specify initial disk bandwidth allocation values for a virtual machine in its configuration file. You may also modify disk bandwidth allocation parameters dynamically using the VMware Management Interface, the console operating system's `procfs` interface or the Perl API.

Reasonable defaults are used automatically when you do not specify parameters explicitly. Information about current disk bandwidth allocations and other status is available via the management interface, the console operating system's `procfs` interface and the Perl API.

### Allocation Policy

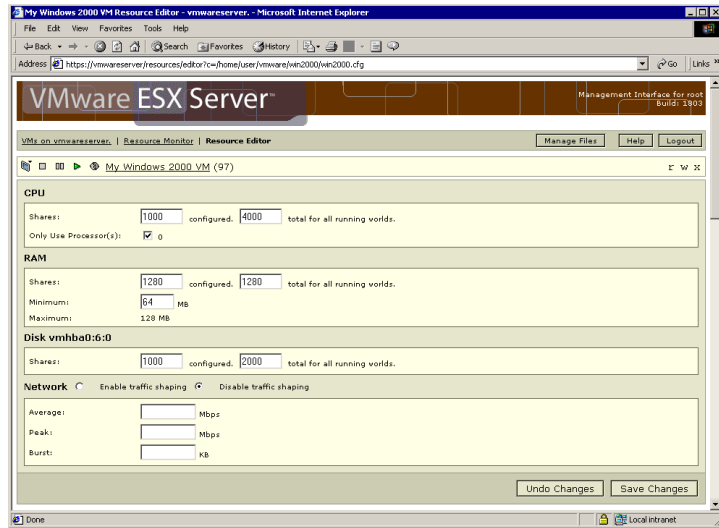
ESX Server uses a modified proportional-share allocation policy for controlling disk bandwidth per virtual machine. This policy attempts to control the disk bandwidth used by a virtual machine to access a disk while also trying to maximize throughput to the disk.

Disk bandwidth shares entitle a virtual machine to a fraction of the bandwidth to a disk. For example, a virtual machine that has twice as many shares as another for a particular disk is entitled to consume twice as much bandwidth to the disk, provided that they are both actively issuing commands to the disk.

Bandwidth consumed by a virtual machine is represented in consumption units. Every SCSI command issued to the disk effectively consumes one unit by default and additional units proportional to the size of the data transfer associated with the command.

Throughput to the disk is maximized through the use of a scheduling quantum for disk requests from a virtual machine to a disk. A virtual machine is allowed to issue a number of requests to a disk (the scheduling quantum) without being preempted by another virtual machine. The issuing of a multiple requests without preemption is applicable only if these requests access sequential sectors on the disk.

### Managing Disk Bandwidth from the Management Interface



To change disk bandwidth settings from the management interface, you must be logged in as root and the virtual machine must be running. Click **Monitor Resources** on the Overview page, then click **Edit Resources** under the name of the virtual machine you want to change. You can edit both the number of shares for the virtual machine you are changing and the total number of shares used on the ESX Server computer.

Enter the desired settings, then click **Save Changes**.

### Configuration File Options

If you edit a virtual machine's configuration file by hand, use the following formats to control disk bandwidth allocation for the virtual machine. You may edit the configuration file using a text editor on the console operating system or through the management interface. To use the text editor in the management interface, go to the virtual machine's Edit Configuration page and click **Use Text Editor**.

```
scsi0:1.name = <fsname>:<diskname>.disk
```

This is the standard format for specifying the VMFS file underlying a virtual disk.

```
sched.disk.shares.<fsname> = <nshares>
```

This configuration option specifies that the initial disk bandwidth share allocation for a virtual machine for the disk containing the VMFS file system <fsname> to be

<nshares> shares. The valid range of values for <nshares> is 0 to 100000, enabling a large range of allocation ratios. If the number of shares for a disk is not specified, the default allocation is 1000.

**Note:** It is important to use the same name when you specify the virtual disk name and the shares for that disk. If <fsname> is used to specify the name of a virtual disk, the same <fsname> must be used to specify the shares. If a fully qualified set of numbers is used to specify the virtual disk name (for example, `vmhba0:5:0`), then the same set of numbers should be used to specify <fsname> when you are setting the number of shares.

**Note:** It is possible for a configuration file to have multiple lines specifying the number of shares. If this happens, the value specified in the last of those lines is used.

### Configuration File Examples

```
scsi0.virtualdev = vmxbuslogic
scsi0:1.present = TRUE
scsi0:1.name = rootdiskfs:rh6.2.dsk
scsi0:1.mode = persistent
sched.disk.shares.rootdiskfs = 800

scsi0:2.present = TRUE
scsi0:2.name = scratchfs:scratch1.dsk
sched.disk.shares.scratchfs = 400
```

In the example above, the first four lines in the first group and the first two lines in the second group are present in the configuration file before you make your changes. The final line in each group is the added line to specify the disk bandwidth allocation. As described above, check the value of <fsname> in the line specifying the VMFS file and use the same value in the line specifying the disk bandwidth allocation. In the first group of lines in the example, that value is `rootdiskfs`; in the second group of lines, it is `scratchfs`.

## Managing Disk Bandwidth from the Console Operating System

Use the following guidelines for the console operating system commands to monitor and manage allocation of disk bandwidth on an ESX Server computer.

```
/proc/VMware/vm/<id>/disk/vmhba<x:y:z>
```

Reading from this file reports the number of disk bandwidth shares allocated to the virtual machine identified by <id> for the disk identified by `vmhba<x:y:z>`. It also reports disk usage statistics.

Writing a number `<nshares>` to this file changes the number of disk bandwidth shares allocated to the virtual machine identified by `<id>` to `<nshares>`. The valid range of values for `<nshares>` is 0 to 100000.

# 10

## **Glossary**

# Glossary

**Append mode** — When software running in the virtual machine writes to a disk used in append mode, the changes appear to be written to the disk. In fact, however, they are stored in a temporary file (.REDO). If a system administrator deletes this redo-log file, the virtual machine returns to the state it was in the last time it was used in persistent mode.

**Configuration** — See Virtual machine configuration file.

**Console operating system** — An operating system that runs on the physical computer to provide an interface to start up and administer your virtual machines. It is managed by the VMkernel.

See also Guest operating system.

**Disk mode** — A property of a virtual disk that defines its external behavior but is completely invisible to the guest operating system. There are four modes: persistent (changes to the disk are always preserved across sessions), nonpersistent (changes are never preserved), undoable (changes are preserved at the user's discretion) and append (similar to undoable, but the changes are preserved until a system administrator deletes the redo-log file). Disk modes may be changed from the VMware Management Interface.

**Guest operating system** — An operating system that runs inside a virtual machine.

**Nonpersistent mode** — All disk writes issued by software running inside a virtual machine with a nonpersistent disk appear to be written to disk, but are in fact discarded after the session is powered down. As a result, a disk in nonpersistent mode is not modified by ESX Server.

**Persistent mode** — All disk writes issued by software running inside a virtual machine are immediately and permanently written to a persistent virtual disk. As a result, a disk in persistent mode behaves like a conventional disk drive on a physical computer.

**Root** — The administrator logs in to the VMware Management Interface and the console operating system with a user name of root.

**Undoable mode** — All writes to an undoable disk issued by software running inside the virtual machines appear to be written to the disk, but are in fact stored in a temporary file (.REDO) for the duration of the session. When the virtual machine is powered down, the user is given three choices: 1) permanently apply all changes to

the disk; 2) discard the changes, thus restoring the disk to its previous state; or 3) keep the changes, so that further changes from future sessions can be added to the log.

**Virtual disk** — A virtual disk is a file on a file system accessible from the server. To a guest operating system, it appears to be a physical disk drive. This file can be on the server where the virtual machine is running or on a remote file system.

**Virtual machine** — A virtualized x86 PC environment on which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same server machine concurrently.

**Virtual machine configuration** — The specification of what virtual devices (disks, memory size, etc.) are present in a virtual machine and how they are mapped to files and devices on the physical computer.

**Virtual machine configuration file** — A file containing a virtual machine configuration. It is created when you set up a virtual machine. It may be modified from the VMware Management Interface or by editing the file in a text editor.





# A

## **Appendix A: I/O Adapter Compatibility Guide**

# I/O Adapter Compatibility Guide

VMware ESX Server has an architecture that delivers high performance I/O for PCI-based SCSI, Fibre Channel, Ethernet and Gigabit Ethernet adapters, as well as internal RAID controllers. These high performance devices are accessed directly through device drivers in the ESX Server and not through a host operating system as with VMware Workstation and GSX Server products.

## Currently Supported Device Families

This appendix to the *VMware ESX Server Version 1.5 User's Manual* provides the latest available information on supported devices. Updates are posted to the VMware Web site at [www.vmware.com/pdf/esx\\_io\\_devices\\_15.pdf](http://www.vmware.com/pdf/esx_io_devices_15.pdf). VMware currently has ESX Server device drivers available that support the following families of adapters.

### SCSI Adapters

- Adaptec SCSI adapters
- Mylex (Buslogic) SCSI adapters
- LSI Logic (Symbios, NCR) chip set based SCSI adapters

### Fibre Channel Adapters (SCSI protocol support only)

- Emulex adapters
- QLogic adapters

### Internal RAID Controllers

- Compaq RAID controllers
- Dell RAID controllers
- IBM RAID controllers
- Mylex DAC960 RAID controllers

### Ethernet NICs

- Intel EEPo Ethernet NICs
- 3Com EtherLink PCI III/XL

### Gigabit Ethernet NICs

- Alteon Websystems AceNIC and compatible Gigabit Ethernet NICs
- Broadcom NetXtreme BCM5700 and compatible
- Intel e1000 and compatible

VMware may add support for drivers and devices between releases of the product; check the VMware Web site for current information.

The ESX Server device drivers deliver high performance device I/O. Disk and Ethernet devices that are not supported by ESX Server drivers may work using console operating system based device I/O. Console operating system I/O performance is significantly slower than that of ESX Server device drivers. VMware discourages using console operating system devices for production deployment. They are intended to be used for migration and similar purposes.

The detailed list below shows actual vendor chip sets and adapters that VMware believes are compatible with the currently supported drivers. Although we have been careful in compiling the list, we have not tested all of these devices and cannot warrant that they all work. There may also be devices that are not listed but that will work with these device drivers.

Please contact VMware with any questions about current and planned device support.

### Linux Driver Compatibility

While the ESX Server itself is not derived from Linux, many ESX Server device drivers are based on Linux driver source code. This enables VMware to more easily support a wide range of high performance devices. VMware typically modifies these drivers for one or more of the following reasons:

- To make the driver compatible with ESX Server
- To tune the driver for performance
- To add I/O resource governing or QoS support to the driver
- To fix generic bugs in the driver

It is not possible to simply load existing Linux device drivers into ESX Server.

Changes to the driver source are contributed back to the Linux community.

### VMware Certification

VMware certifies that specific systems and components are compatible with ESX Server. Through its Preferred Hardware Partner Program, it works with leading server vendors to ensure that appropriate configurations of their current and future server products are certified with ESX Server products.

### Adaptec SCSI Adapters

The ESX Server Adaptec driver is based on the Linux aic7xxx version 5.1.28 driver. The following PCI Adaptec SCSI adapters and motherboard chip set devices should work as ESX Server adapters.

#### SCSI Adapters

- AHA-2910B
- AHA-2920 (C)
- AHA-2930 (U/U2/CU)
- AHA-2940 (W/U/UW/UW-PRO/A/AU/U2W/U2/U2B/U2BOEM)
- AHA-2944 (D/WD/UD/UWD)
- AHA-2950 (U2/U2B/U2W)
- AHA-3940 (W/U/UW/AUW/U2W/U2B)
- AHA-3950 (U2B/U2D)
- AHA-3960D
- AHA-3985 (U/W/UW)
- AHA-19160Ultra160
- AHA-29160Ultra160
- AHA-39160Ultra160

#### Motherboard Chip Sets

- AIC-3860
- AIC-777x
- AIC-785x
- AIC-786x
- AIC-787x
- AIC-788x
- AIC-789x

#### Adaptec SCSI Adapters and Chip Sets NOT Supported

The following Adaptec SCSI Adapters will not work with this ESX Server driver. They may work as lower performance console operating system devices.

- AHA-2920 w/Future Domain chip set
- AAA-13XRAID Adapter

- AAA-113xRAID Port Card
- AIC-7810(motherboard chip set)
- AHA-174x
- AHA-1542
- AHA-152x
- AIC-6260
- AIC-6360

### **Mylex (Buslogic) SCSI Adapters**

ESX Server's Mylex (Buslogic) driver is based on the Linux BusLogic version 2.1.15 driver. The following PCI Mylex (Buslogic) MultiMaster and Flashpoint SCSI adapters and motherboard chip set devices should work as ESX Server adapters.

Buslogic was acquired by Mylex, which was then acquired by IBM. However, the drivers for these adapters are still generally referred to as Buslogic drivers. For more information about Mylex products see [www.mylex.com](http://www.mylex.com).

### **FlashPoint Series PCI Host Adapters**

- FlashPoint LT (BT-930) Ultra SCSI-3
- FlashPoint LT (BT-930R) Ultra SCSI-3 with RAIDPlus
- FlashPoint LT (BT-920) Ultra SCSI-3 (BT-930 without BIOS)
- FlashPoint DL (BT-932) Dual Channel Ultra SCSI-3
- FlashPoint DL (BT-932R) Dual Channel - Ultra SCSI-3 with RAIDPlus
- FlashPoint LW (BT-950R) Wide Ultra SCSI-3 with RAIDPlus
- FlashPoint DW (BT-952) Dual Channel Wide Ultra SCSI-3
- FlashPoint DW (BT-952R) Dual Channel Wide Ultra-SCSI-3 with RAIDPlus

### **MultiMaster "W" Series Host Adapters**

- BT-948 PCI Ultra SCSI-3
- BT-958 PCI Wide Ultra SCSI-3
- BT-958D PCI Wide Differential Ultra SCSI-3

### **Buslogic MultiMaster "C" Series Host Adapters**

- BT-946C PCI Fast SCSI-2
- BT-956C PCI Wide Fast SCSI-2
- BT-956CD PCI Wide Differential Fast SCSI-2

### LSI Logic (Symbios, NCR) Based SCSI Adapters

Most SCSI adapters based on the LSI Logic Symbios (formerly NCR) 53c8xx family of chip sets are supported as ESX Server devices. The ESX Server uses two different drivers to support the device family, one based on the Linux ncr53c8xx version 3.4.3b driver and the other on the sym53c8xx version 1.7.3 driver. LSI Logic's Symbios product division was formerly NCR Microelectronics Products Division. Older products may have either NCR or Symbios (SYM) part number prefixes; otherwise the part numbers are interchangeable. The following chip sets and adapters should work as ESX Server devices.

#### Supported Symbios Chip Sets

- SYM53C810
- SYM53C810A
- SYM53C815
- SYM53C820
- SYM53C825
- SYM53C825A
- SYM53C860
- SYM53C875
- SYM53C876
- SYM53C895
- SYM53C895A
- SYM53C896
- SYM53C897
- SYM53C1510D

#### Supported Symbios based SCSI Adapters

##### Model/Type — Chip Set

- SYM20810 32 bit PCI-to-Fast SCSI — SYM53C810A
- SYM20811 32 bit PCI-to-Fast SCSI — SYM53C810A
- SYM20860 32 bit PCI to Ultra SCSI — SYM53C860
- SYM21002 32 bit PCI-to-Ultra2 SCSI — SYM53C896
- SYM22801 PCI-to-Dual Ultra SCSI — SYM53C876
- SYM22802 PCI-to-Ultra SCSI — SYM53C876

- SYM22902 Ultra2 MiniHAB — SYM53C895A/SYM53C895
- SYM22910 PCI-to-Dual Ultra2 SCSI — SYM53C896
- 815XS — SYM53C815
- 8100S — SYM53C810
- SYM8150 — SYM53C815
- SYM8251 — SYM53C825
- SYM8600SP — SYM53C860
- SYM8750SP — SYM53C875
- SYM8751D — SYM53C875
- SYM8751SPE — SYM53C875
- SYM8951U — SYM53C895
- SYM8952U — SYM53C895A/SYM53C895
- SYM8953U — SYM53C895A
- SYM53C1010 — Ultra160
- SYM53C1010\_66 — Ultra160

Third-party SCSI adapters from Compaq/DEC, Gigabyte, Promise Technology and Tyan should also work with the ESX Server NCR driver.

### Chip Sets NOT Supported

- NCR 5380
- NCR 53c400
- NCR 53c810/820/720
- NCR 53c700/710/700-66
- NCR 53C875
- NCR 53C876

### Emulex Fibre Channel Adapters

The ESX Server driver is based on the Linux port of the Emulex version lpfcdd version 4.12c driver. This adapter has been tested with ESX Server adapter only in point-to-point configurations. Most fabric capabilities such as fabric login, as well as loop or switched configurations with multiple hosts, skipped LUNs or high-number targets, have not been tested.

- LP850
- LP7000 series
- LP8000 series
- LP9000 series

### QLogic Fibre Channel Adapters

The ESX Server driver is based on the Linux port of the QLogic qla2x00 version 4.46.12b driver. This adapter has been tested with ESX Server only in point-to-point configurations. Most fabric capabilities such as fabric login, as well as loop or switched configurations with multiple hosts, skipped LUNs or high-number targets, have not been tested.

- QLA-2100
- QLA-2200
- QLA-2300

### Compaq RAID Controllers

The ESX Server driver is based on the Compaq SMART2 v 2.4.5 driver, for everything except Smart-5 devices, which are based on the Compaq CCISS Driver v 2.4.6.

- IDA, IDA-2, IAES
- SMART
- SMART-2/E
- SMART-2 (SMART-2/P, SMART-2SL, Smart Array 3200, Smart Array 3100ES, Smart Array 221)
- SMART-4 (Integrated Array, Smart Array 4200, Smart Array 4250ES, Smart Array 431)
- SMART-5 (Smart Array 5300 series, Smart Array 5i, Smart Array 532)



### Dell PercRAID RAID Controllers

VMware ESX Server supports two classes of PercRAID branded controllers. Some are based on Adaptec RAID chipsets and some on American Megatrends, Inc. (AMI) MegaRAID chipsets.

The ESX Server driver for Adaptec-based PercRAID controllers is based on the Linux aacraid version 2.1.5 driver.

- PERC 2/QC
- PERC 3/Si (PowerEdge 2450 onboard RAID)
- PERC 3/Di (PowerEdge 2550 and 4400 onboard RAID)

The ESX Server driver for AMI-based PercRAID controllers is based on the Linux megaraid version 1.18 driver.

- PERC 2/DC
- PERC 3/DCL

### IBM ServeRAID RAID Controllers

The ESX Server driver is based on the Linux ips version 4.80.26 driver.

- ServeRAID/4L
- ServeRAID-4Lx
- ServeRAID-4H
- ServeRAID-4Mx
- ServeRAID-3H

### Mylex DAC960 RAID Controllers

The ESX Server driver is based on the Linux DAC960 version 2.4.10 driver. Specific AcceleRAID and eXtremeRAID controllers are also based on DAC960-compatible controllers.

- DAC960P/PD/PJ
- AcceleRAID 250, 200, 150
- eXtremeRAID 1100

### Intel EPro Family Ethernet NICs

The default ESX Server driver for EPro family 10Mb and 10/100 NICs is based on the Intel-supplied e100 "Intel(R) PRO/100 Fast Ethernet Adapter" version 1.6.29 driver. This driver supports the Intel i82557, i82558 and i82559 chips. This is a comprehensive

listing of Intel and OEM models which have been based on these chip sets. You should check the specific chip set used in your card for compatibility.

- Intel(R) PRO/100B PCI Adapter (TX)
- Intel(R) PRO/100B PCI Adapter (T4)
- Intel(R) PRO/10+ PCI Adapter
- Intel(R) PRO/100 WfM PCI Adapter
- Intel(R) 82557-based Integrated Ethernet PCI (10/100)
- Intel(R) PRO/100B PCI Adapter (T4)
- Intel(R) PRO/10+ PCI Adapter
- Intel(R) PRO/100 WfM PCI Adapter
- Intel(R) 82557-based Integrated Ethernet PCI (10/100)
- Intel(R) 82558-based Integrated Ethernet
- Intel(R) PRO/100+ Management Adapter
- Intel(R) PRO/100+ Adapter
- Intel(R) PRO/100+ Management Adapter
- Intel(R) PRO/100+ Server Adapter
- Intel(R) PRO/100+ Server Adapter (PILA8470B)
- Intel(R) PRO/100 S Server Adapter
- Intel(R) PRO/100 Dual Port Server Adapter
- Intel(R) PRO/100 S Dual Port Server Adapter
- Intel(R) PRO/100+ Dual Port Server Adapter
- Intel(R) PRO/100+ Management Adapter with Alert On LAN\* G Server
- Intel(R) PRO/100 S Server Adapter
- Intel(R) PRO/100 Server Adapter
- Intel(R) PRO/100+ Dual Port Server Adapter
- Intel(R) PRO/100 S Mobile Adapter
- Intel(R) PRO/100 CardBus II
- Intel(R) PRO/100 LAN+Modem56 CardBus II
- Intel(R) PRO/100 SR Mobile Adapter
- Intel(R) PRO/100 S Mobile Combo Adapter

- Intel(R) PRO/100 S Combo Mobile Adapter
- Intel(R) PRO/100 SR Combo Mobile Adapter
- Intel(R) PRO/100 P Mobile Adapter
- Intel(R) PRO/100 SP Mobile Adapter
- Intel(R) PRO/100 P Mobile Adapter
- Intel(R) PRO/100 Network Connection
- Intel(R) PRO/100 P Mobile Combo Adapter
- Intel(R) PRO/100 SP Mobile Combo Adapter
- Intel(R) PRO/100+ Mini PCI
- Intel(R) PRO/100 P Mobile Combo Adapter
- Intel(R) PRO/100+ Mini PCI
- Intel(R) 82559 Fast Ethernet LAN on Motherboard
- Intel(R) 82559 Fast Ethernet LOM with Alert on LAN
- Intel(R) PRO/100 S Network Connection
- Intel(R) PRO/100 Network Connection
- Compaq Fast Ethernet Server Adapter
- Intel(R) PRO/100 VE Desktop Adapter
- Intel(R) PRO/100 VM Desktop Adapter
- Intel(R) PRO/100 VE Network Connection PLC LOM
- Intel(R) PRO/100 VE Network Connection
- Intel(R) PRO/100 VM Network Connection
- Intel(R) PRO/100 P Mobile Combo Adapter
- Intel(R) PRO/100 P Mobile Adapter
- Intel(R) PRO/100 Network Connection
- Intel(R) PRO/100 VE Network Connection
- Intel(R) PRO/100 VM Network Connection
- Intel(R) 8255x-based Ethernet Adapter

### 3Com EtherLink PCI III/XL Series Ethernet NICs

ESX Server supports many 3Com Ethernet NICs. The ESX Server driver includes two drivers, one based on the Linux 3c90x version 1.0.0c driver, and the other based on the Linux 3C990-x version 1.0.0b. The following 3Com NICs should work as ESX Server devices.

#### EtherLink 10/100 PCI NICs

- 3C905C Family and 3C920 ASICs — EtherLink 10/100 PCI including the -TX and -TX-M
- 3C905B Family and 3C918 ASICs — EtherLink 10/100 PCI including the -TX -TX-M and -TX-NM
- 3C905B-COMBO — EtherLink 10/100 PCI COMBO
- 3C905B-T4 — EtherLink 10/100 PCI T4

#### EtherLink Server 10/100 PCI NICs

- 3C980C-TX — EtherLink Server 10/100 PCI
- 3C980B-TX — EtherLink Server 10/100 PCI
- 3C980-TX — EtherLink Server 10/100 PCI

#### EtherLink 100 PCI NIC

- 3C905B-FX — EtherLink 100 PCI Fiber

#### EtherLink 10 PCI NICs

- 3C900B-TPO — EtherLink 10 PCI TPO
- 3C900B-TPC — EtherLink 10 PCI TPC
- 3C900B-COMBO — EtherLink 10 PCI COMBO
- 3C900B-FL — EtherLink 10 PCI Fiber

In addition all cards based on the 3cr990-x card should be compatible with ESX Server.

### Alteon AceNIC and Compatible Gigabit Ethernet NICs

ESX Server supports Gigabit Ethernet NICs based on the Alteon WebSystems Tigon I and Tigon II chip sets. The ESX Server driver is based on the Linux AceNIC version v0.85driver. The following NICs should work as ESX Server devices.

- Alteon — AceNIC 1000BASE-SX Fiber
- Alteon — AceNIC 10/100/1000BASE-T Twisted Pair
- 3Com — Gigabit EtherLink Server NIC 3C985

- Farallon — PN9000sx
- Netgear — GA620 Gigabit Ethernet Card
- Netgear — GA620T Copper Gigabit Ethernet Card
- Digital (Compaq) — PCI-to-Gigabit Ethernet Adapter DEGPA-SA

The ESX Server driver does not currently support the jumbo frames and checksum offloading capabilities of these NICs.

### **Broadcom Gigabit Ethernet NICs**

The ESX Server driver for Broadcom Gigabit Ethernet cards is based on the Broadcom 5700 driver for Linux version 1.4.5 driver. Broadcom based drivers are now the embedded Gigabit card in multiple vendor systems, so specific part numbers may vary.

- Broadcom NetXtreme BCM 5700

### **Intel Gigabit Ethernet NICs**

The ESX Server driver for Intel Pro 1000 drivers Gigabit Ethernet cards is based on the Linux v4.0.7 version driver.

- Intel(R) PRO/1000 Network Driver



# B

## **Appendix B: The OpenSSL Toolkit License**

# The OpenSSL Toolkit License

The licence agreement for the usage of the OpenSSL utility included with VMware ESX Server is as follows:

## License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### OpenSSL License

Copyright © 1998-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"



THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

# Index

## A

- Access
  - SNMP controls 129
  - to configuration file 193
- Accessibility
  - of virtual disks 210
  - VMFS 48, 56
- Affinity set 235
- API
  - Perl 142, 147
- Append
  - disk mode 62, 262
- Authentication 193

## C

- CD-ROM
  - attaching to image file 63
- Clustering
  - sharing virtual disks 210
- Color depth 63
- Command
  - passing from console operating system to guest 147
- Commit 202
- Communication
  - from console operating system to guest 147
- Configuration
  - server 33
  - SNMP agent 129
  - virtual machine 60, 68, 99, 181
- Console operating system 28, 171, 205
  - file size limits 207
- Copy
  - in file manager 101
  - text 119
- Core dump 46, 52
- cp 205
- CPU
  - affinity set 235
  - monitoring with SNMP 126

- scheduling virtual machine use of 234

- Cut
  - in file manager 101
  - text 119

## D

- Debug monitor 63
- DHCP 171
- Directories
  - managing remotely 99
- Directory
  - creating 104
- Disk mode 61, 108, 183, 262
  - append 61, 62, 262
  - nonpersistent 61, 62, 262
  - persistent 61, 262
  - undoable 61, 62, 262
- Disks
  - monitoring with SNMP 126
  - mounting vmfs file systems 206
  - SCSI target IDs 208
  - using vmkfstools to manipulate files on 199
- Display name
  - for virtual machine 60

## E

- Edit configuration
  - open from file manager 101
- Export
  - virtual machine 118, 201

## F

- Fibre Channel 17
- File manager 99
  - compatible Web browsers 100
  - cut, copy and paste 101
  - renaming files and folders 102
  - setting permissions 102
- Files
  - managing remotely 99

- size limits on console operating system 207
- size reported on VMFS file systems 207

- Filters
  - network 253

- findnic 220

- Floppy disk image file 63

- Folder
  - creating 104

- Format
  - VMFS partition 55

- FreeBSD
  - installing VMware Tools in 78
  - sample configuration file 164

- FreeBSD 4.5
  - installing as guest operating system 164

- FTP 205
  - TCP/IP port 195

## G

- Gigabit Ethernet 62
- GSX Server 184
  - migrating virtual machines 71
- Guest operating system 262
  - and SNMP 132
  - FreeBSD 4.5 164
  - guest operating system service 167
  - guestd 167
  - installing 70, 150
  - Red Hat Linux 6.2 160
  - Red Hat Linux 7.0 158
  - Red Hat Linux 7.1 156
  - Red Hat Linux 7.2 156
  - Red Hat Linux 7.3 154
  - setting in configuration 60
  - supported systems 20
  - SuSE Linux 7.3 162
  - Windows 2000 152
  - Windows NT 153
- Guest operating system service 144

- Linux reboot commands 146
- shutting down and restarting a virtual machine 145

- guestsd 167

## H

- Hardware
  - installing on server 86
- Heartbeat
  - monitoring with SNMP 127
- HTTP
  - TCP/IP port 195
- HTTPS
  - TCP/IP port 195

## I

- ID
  - virtual machine 98
- Import
  - virtual machine 201
- Installation
  - of guest operating system 70, 150
  - of hardware on server 86
  - of server software 28
  - of software in a virtual machine 119
  - of the SNMP agent 127
- Interrupt clustering
  - and network performance 228
  - parameters 228
- ISO disc image file 63

## K

- Kerberos 193

## L

- LDAP 193
- License 40
- Linux
  - installing VMware Tools in 76
- Logical name
  - assigning to VMFS partition 56

## M

- MAC address
  - setting manually 217

- machine.id 147

## Management

- CPU resources 234
- memory resources 239
- network bandwidth 253
- registering virtual machines 67, 79
- remote management software 79
- setting MIME type in browser 111, 112
- TCP/IP ports used 194
- VMware Management Interface 94

## Memory

- dynamic allocation 240
- maximum size 239
- minimum size 239
- monitoring with SNMP 126
- reclaiming unused 241
- resource management 239
- server requirements 17
- shares 239
- size for virtual machine 61

## Message

- passing from console operating system to guest 147

- MIME type, setting 111, 112

- mount-vmfs 206

## N

- NDIS.SYS 75

## Network

- adapter allocation 36
- bandwidth management 253
- configuring on virtual machine 182
- driver in virtual machine 71
- locating adapter in use 220
- MAC address 217
- monitoring with SNMP 126
- performance tuning 228
- setting virtual adapter to promiscuous mode 222
- shaping traffic 254
- sharing adapters 224
- using Gigabit Ethernet 62
- virtual 224

- vmnet adapter 62

- vmnic adapter 62

## Network driver

- manual speed settings 221
- vlan 62
- vmxnet 62

- NewsGroups 22

- NFS 205

- nfshaper 177

- NIS 193

- Nonpersistent
  - disk mode 62, 262

## O

- OpenSSL Toolkit License 280

## P

- PAM 193

- Partitioning 46, 51

## Paste

- in file manager 101
- text 119

## Performance

- network 228

- Perl API 142, 147

- Permissions 194
  - changing in file manager 102

## Persistent

- disk mode 61, 262

## portmap

- TCP/IP port 195

## Processor

- affinity set 235
- scheduling virtual machine use of 234

- Promiscuous mode 222

## R

## RAID 17

- device allocation 36
- file system management 199
- multiple function adapters 36
- partitioning 46, 51
- shared 36

## Index

- Red Hat Linux 6.2
  - installing as guest operating system 160
- Red Hat Linux 7.0
  - installing as guest operating system 158
- Red Hat Linux 7.1
  - installing as guest operating system 156
- Red Hat Linux 7.2
  - installing as guest operating system 156
- Red Hat Linux 7.3
  - installing as guest operating system 154
- Register
  - virtual machines 67, 79
- Remote console 96
  - color depth setting 63
  - installing 81
  - starting 114
  - using 114
- Remote management 79
- Remote management workstation
  - system requirements 19
- Rename
  - using the file manager 102
- Reset 96
- Restart
  - using guest operating system service 145
- Resume 96, 120, 190
  - repeatable 191
- Root 262
- S**
- scp 205
- SCSI 17, 210
  - configuring on virtual machine 182
  - device allocation 36
  - disk partitioning 46, 51
  - file system management 199
  - multiple function adapters 36
  - shared 36
  - target IDs 208
- SCSI disk or RAID 46, 51
- Security 42, 193
  - SNMP 132
- Security certificate
  - installing 83
- Serial number 40
- Server
  - shutting down 122
- Setup Wizard 33
- Shaping network traffic 254
- Shares
  - memory 239
  - of CPU time 234
- Sharing
  - virtual disks 210
- sharing the SCSI bus 210
- Shut down
  - server 122
  - using guest operating system service 145
  - virtual machine 121
- Sizing
  - memory 249
- sizing for the server 249
- SleepWhenIdle 186
- SMBIOS
  - modifying the UUID 187
- SNMP 125
  - access controls 129
  - and guest operating systems 132
  - and VMware Tools 127
  - configuring management software 131
  - configuring the agent 129
  - installing the agent 127
  - location of the VMware subtree 125
  - security 132
  - traps 127
  - variables 132
- Software
  - installing in a virtual machine 119
- Speed
  - setting for network driver 221
- SSH
  - TCP/IP port 195
- String
  - passing from console operating system to guest 147
- SuSE Linux 7.3
  - installing as a guest operating system 162
- Suspend 96, 120, 190
  - location of suspended state file 63
- Swap file
  - for ESX Server memory management 48, 57
- System requirements 17
  - remote management workstation 19
  - server 17
- T**
- TCP/IP ports
  - used for management access 194
- Technical support 22
- Telnet
  - TCP/IP port 195
- Time
  - synchronizing between guest and console operating systems 144
- U**
- Undoable
  - disk mode 62, 262
- Upgrading
  - from previous version of ESX Server 87
- User accounts 32
- UUID
  - modifying 187
- V**
- Variables
  - SNMP 132
- Virtual disk 62

- exporting 118
    - on console operating system 184
    - sharing 210
  - Virtual machine
    - configuring 181
    - creating 59
    - deleting from VMware Management Interface 106
    - display name 60
    - exporting 201
    - ID number 98
    - importing 201
    - monitoring with SNMP 126
    - registering 67, 79
    - shutting down 121
    - suspending and resuming 190
  - Virtual Machine Wizard 59
  - Virtual network 224
  - vlane network driver 62
  - VMFS 47, 182, 199
    - formatting partition 55
    - mounting 205, 206
    - naming 56, 185, 203, 205
  - VMkernel
    - device modules 173, 174
    - devices 182
    - loading and unloading 173
  - vmkfstools 199
  - vmkload\_mod 174
  - vmkloader 173
  - vm-list 79, 194
  - vmnet network adapter 62
  - vmnic network adapter 62
  - VMware guest operating system service
    - VMware Tools 144
  - VMware Management Interface
    - controls 95
    - deleting a virtual machine 106
  - VMware Tools
    - and SNMP 127
    - installing 70
    - settings 117
    - starting automatically in
      - Linux guest 77
      - VMware guest operating system service 144
  - VMware Workstation 184
    - migrating virtual machines 71
  - vmware-authd 193
    - TCP/IP port 195
  - vmxnet network driver 62
  - vmxnet.sys 75
- ## W
- Web browser
    - and file manager 100
    - and the console operating system 171
    - and the VMware Management Interface 94
  - Windows 2000
    - installing as guest operating system 152
    - installing VMware Tools in 73
  - Windows NT
    - installing as guest operating system 153
    - installing VMware Tools in 74
- ## X
- X server 162
    - and the console operating system 171